1995

Security issues in electronic data interchange (EDI) systems

Nitin Devikar
University of Wollongong

SECURITY ISSUES IN ELECTRONIC DATA INTERCHANGE (EDI) SYSTEMS

A thesis submitted in partial fulfilment of the

requirements for the award of the degree

Master of Science (Honors)

from

UNIVERSITY OF WOLLONGONG

by

Nitin Devikar B.E

Department of Computer Science

1995

Abstract

Currently there is limited security offered in the Electronic Data Interchange (EDI) systems. Due to the growth of global market, Electronic Data Interchange is becoming an important tool for improving business prospects and hence becoming a target for fraud and misuse of information. This thesis attempts to provide security enhancements in the EDI systems. A model of the EDI system, the *Direct Store Delivery System* is described with security features added for global use. The model uses a Third Party Service Provider providing Message Handling Systems for communication between the trading partners. This thesis describes the security enhancement in the EDI messages using the UN/EDIFACT standard of formatting the EDI messages with the inclusion of certificates, digital signatures in the messages without changing the syntax of the EDI message. Also, a proposal to use X.500 Directory Services standards for global authentication is described along with other network security services. All these security services are included in the Application layer of the OSI reference model and are transparent to the user. As a result of the proposal, the security services can be implemented on a global basis as a step towards an open-edi system.

Acknowledgment

I would like to take this opportunity to thank my supervisors Prof. Jennifer Seberry and Dr. Yuliang Zheng for providing me with all the support and encouragement I needed for the successful completion of this work. They were always there to clear up doubts and provide suggestions for the improvement of my work.

I would also like to thank the support staff of Computer Science department and the Center for Computer Security Research for their assistance.

Thanks are also due to Mr. Fernando Lagrana of the International Telecommunication Union for providing the complimentary copy of X.500 Directory Services Blue Book and Dr. Andrew Waugh of CSIRO for providing me with the latest update of the X.509 standards.

I am also thankful to all my friends for their support during the year.

I am grateful to my parents for their solid support and blessings, without which I would not have been able to pursue any higher studies.

Publications Arising Out of Thesis

A paper co-authored by Nitin Devikar and Dr. Yuliang Zheng titled "Security Enhanced Direct Store Delivery System" appeared in the Proceedings of the Eighteenth Australasian Computer Science Conference, Volume 17, Number 1, pp 130-135, ISSN 0157-3055, 1995.

Contents

List of Figures

Chapter 1

Introduction

This chapter gives a brief introduction to the basic issues of network security, Electronic Data Interchange (EDI) and EDI security.

1.1 Introduction

During the 1990s, there has been a significant rise in the commercial use of computer networks. Their implications and effectiveness in business have been felt worldwide, allowing organizations to eliminate "... *barriers of geography and time on service and co-ordination*" [48] and "... *reach out beyond the boundaries of the organization to the premises of the customers, suppliers, government agencies and others*"[49]. These telecommunication capabilities have provided business with increased potential and ease of global trade by bringing fundamental changes in the organizational procedures. The growing number of electronic linkages between traders has produced dramatic effects on the inter-organizational relationships and industry structure.

Industries, as well as government agencies view Electronic Data Interchange

(EDI) as the emerging technology to support this growth. EDI is often viewed as a way of replacing the traditional paper documents (e.g. purchase order forms, shipping forms, invoices, financial documents etc.) with electronic ones, and replacing conventional methods of transmitting such documents (e.g. mail, telephone, facsimile, courier etc.) with electronic transmissions. EDI, however, can also replace manual data entry with electronic data entry (by providing a Universal Product Code) and can also provide a platform for effective business re-engineering. To ensure the inter-operatability between the various EDI systems, they should be independent of any particular hardware or software. In addition, the EDI messages should be conveyed in a structured format. Thus, the primary purpose of EDI, is to provide communication standards that promote the interchange of common business information to facilitate the electronic linkages, without human intervention.

EDI systems have been successfully implemented, often involving multiple business functions (such as shipping and billing), in a number of industries (such as automobile, insurance, groceries etc.). There are obvious advantages in implementing EDI in terms of speed, accuracy and flexibility. However, a major concern embedded in the use of Electronic Data Interchange (EDI) is the ever greater need to protect the information from misuse. Security and privacy have become prominent issues in those public and private sectors which use Electronic Data Interchange. They all rely on communication networks for communicating sensitive, commercial, financial and personal information. As the communication networks are not secure, it is therefore necessary to protect their valuable information both within the communication networks and within the information processors connected to the network. If these concerns are not properly resolved, they threaten to limit the full potential of networking, in

terms of both participation and usefulness.

1.2 Network Security Issues

The use of EDI requires formatting the data in a structured manner and also requires communication networks for transmitting these EDI messages. The users of EDI have the same expectations as users of conventional computer systems. They expect accurate delivery of messages; protection from loss; modification or observation of messages; and reliable service. These are the network equivalents of integrity, secrecy and availability. However, several security problems are inherent in the network access and its use.

1.2.1 Problems in Network Security

In today's environment, networking offers the advantage of sharing important information among the authorized personnel, both inside and outside the organization and cost effectiveness in implementing a network solution. Pfleeger [28] has discussed some reasons for security problems in networks.

Sharing

Due to resources and workload sharing of networks, a greater number of users have the potential to access networked systems than single computers. Since the access is afforded for many systems, the access controls for a single system is inadequate in networked environments.

Complexity of the System

A network combines two or more possibly dissimilar operating systems with mechanisms for interhost connection. Therefore, a network operating system

or control system is likely to be more complex than an operating system for a single computing system. This complexity deters the certification or confidence in the security of a network.

Many Points of Attack

A single computing system is a self contained unit. Access controls on one machine preserves the secrecy of its data. However, when a file is stored in a network host remote from that user, the file may pass through several host machines to get to the user. The administrator of one machine may enforce rigorous security policies, but that administrator does not have any control over the other hosts in a network. Thus the user in a networked system has to trust the access control mechanisms of all these systems.

Unknown Perimeter in a Network

The expandibility of a network also implies uncertainty about the network boundary. One host may be a node on two different networks so that the resources on one network are accessible to the users of the other network as well. Although wide acceptability is an advantage, this unknown and uncontrolled group of potentially malicious users is a security disadvantage. A similar problem occurs when new hosts are added to a network. Every network node must be able to react to the presence of new, and possibly untrustworthy hosts.

1.2.2 Network Security

Since more and more information is conveyed through a computer network, one of the issues concerning security involves protecting information as it is transmitted through the network. There are three major trends leading to an

urgent reassessment and causing the escalation of concerns in communications security [20]. These are :–

- the increasing interconnection of systems and of networks, making any system potentially accessible to a rapidly growing population of known and unknown users;
- The increasing use of computer networks for security-sensitive information e.g. EFT, business data interchange, unclassified but sensitive government information and corporate proprietary information; and
- The increasing ease of engineering a network attack, given the ready availability of increasingly sophisticated technology and the rapidly falling costs of such technology to a would-be attacker.

There are many potential types of attacks on commercial or unclassified government networks. They include financial frauds, theft of telecommunication resources, industrial espionage, illicit eavesdropping for financial or political gain and malicious attacks by intruders. In addition to countering all these attacks the communication's security needs to protect data against accidental exposures. The accidental connection of a sensitive communication session to the wrong address or the accidental failure to properly protect sensitive information may prove as damaging as a successful deliberate attack. As an EDI system often transmits commercial or financial data through networks, this information needs to be protected against network security threats in general.

1.3 Need for EDI Security

The growth of EDI started in small closed user groups, where the trading partners knew and trusted each other. The data being transferred was not

very critical in context (e.g. purchase orders which are not usually subject to fraudulent use). As organizations began to rise along the EDI learning curve they began to understand that the real benefits from EDI results from being able to restructure the existing business processes. EDI provides simplification and improvement of existing business processes and matches them with those of the trading partners. As the technology goes towards an open-EDI, where orders might be accepted from a company with which no trading relationship exists at this time, the security and audit policies must also be upgraded to match this new technology. Nowadays, EDI is increasingly being used for financial transactions and greater security is required in a financial transaction.

Electronic security systems such as Automatic Teller Machines (ATMs) and Society Worldwide for Interbank Financial Transfer (SWIFT) have been around for some years transferring money to and from banks and providing basic security services for their operation. However, Cobb [31] identifies two major differences between the requirements of Electronic Data Interchange and Electronic Funds Transfer (EFTs):

- Existing EFTs are operated and managed by a single enterprise or by a clearly defined closed user groups. EDI, on the other hand, involves multiple independent parties, transferring many different types of transactions between each other. The identification and status of the originator of an EDI transaction will not always be known to the recipient of that transaction.

- Most EFTs today are operated on private networks with restricted access. EDI, however, uses store and forward services from multiple service providers. This means that data will be in *escrow*, during some part of

its transmission, which is outside the direct control of the originator or recipient.

The aim and scope of this thesis is based on the security issues in the Electronic Data Interchange involving multiple trading partners connected via a Value Added Network Service (VAN).

1.4 Aim of the Thesis

EDI transactions can be divided into two distinct generic activities. The primary activity is the creation of a EDI document from internal data. This requires in-house interface software to translate the outgoing messages from (possibly) unstructured, company or application specific formats into the EDI document translation format, e.g. ANSI X12, UN/EDIFACT, and placing the resulting universal documents into an electronic outgoing message with the proper security headers and trailers inserted in the message format. The second activity is the transmission of the standardized EDI document to its recipient. This requires telecommunication software which transmits the now structured message to its internal/external recipient typically using data communication standards as defined in the OSI Reference Model.

The main aim of this thesis is to provide security enhancements in the existing EDI systems. This includes providing security enhancements in the EDI messages using the UN/EDIFACT standards to structure the data and in the communication networks while transmitting the EDI messages.

The current implementations of telecommunication networks for private users require an increasing awareness of network security issues. Within a

single management domain, where all the processing nodes and network links are under the control of the same administration, security is not such a critical issue. However, when the management association takes place across the boundary between two separate management domains, and makes use of the public data networks, security issues should be considered in greater detail. The proposals to counter network security threats are described using the X.400 Message Handling Systems and X.500 Directory Services standards.

1.5 Scope of the Thesis

This thesis presents the background on the communication and security aspects of Electronic Data Interchange. It discusses the security threats in EDI and the need to enhance the security of the present day EDI systems to support the future trend of open-EDI systems. Finally it proposes a model of an EDI system, the *Direct Store Delivery System* to incorporate security services such as authentication; non-repudiation; authorization; delegation and access control which are necessary to ensure secure and smooth operation of the EDI system.

In chapter 2, an overview of EDI is presented along with the specific advantages and means of implementing EDI in an organization. Also, Value Added Network Services (VANS) used to transmit EDI messages in a store and forward manner, are described with their advantages.

In chapter 3, the security issues related to EDI are discussed and evaluation of the threats posed to the EDI system. Some security issues such as cross-vulnerability; multiplicity of standards and password guessing attacks

are highlighted.

In chapter 4, the X.400 and X.500 secure message handling systems standards are explained. The main security services provided by the standards are discussed and their use in the proposed model to provide the security enhancement to the EDI system is described.

In chapter 5, the Direct Store Delivery System, a model of the EDI system is proposed. The model is based on the Just-In-Time (JIT) principle of inventory management.

In chapter 6, the security services provided in an UN/EDIFACT standard of EDI messages are described along with the security enhancement provided in the standard. In particular, the inclusion of digital signatures, certificates for authentication of origin, message integrity in the messages itself without changing the syntax of the message are discussed.

In chapter 7, the basic security services needed to ensure the smooth operation of the proposed system are described. The authentication protocol based on the X.509 standards is presented. Other security services such as user identification; non-repudiation and responsibility are also discussed.

Finally in chapter 8, the solutions given in the proposed model of EDI are discussed and suggestions for further research work are proposed.

In Appendix A, the paper titled "Direct Store Delivery System" is presented.

Chapter 2

Electronic Data Interchange System

This chapter presents an overview on Electronic Data Interchange systems. The basic concepts of Electronic Data Interchange and its advantages are described. In addition, the benefits of using Value Added Network Service in an EDI system are described for communication between trading partners.

2.1 Basic Elements of Electronic Data Interchange

Electronic Data Interchange (EDI) is the movement of business data electronically within or between firms in a structured, computer processable data format that permits data to be transferred without rekeying from an application in one location to an application in another location [23]. In the traditional paper-based flow of information, manual data entry is performed at each step in the process. In addition, a comparison of purchase orders, receiving of notices and invoices are also required to be done manually. This contributes to the higher

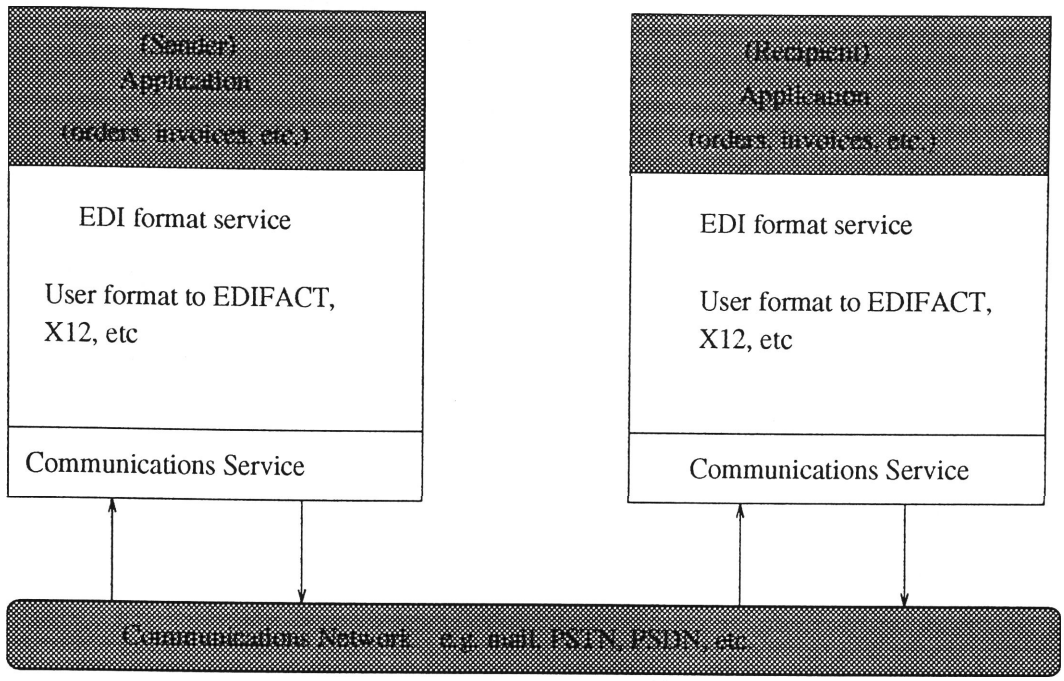


Figure 2.1: Basic Elements in EDI

cost of transaction processing and the continued involvement of the end user in the overall process. These two manual processes are eliminated with the substitution of electronic methods such as EDI. In an EDI system the computer transfer can be direct, with two companies using an agreed data protocol, or it can be performed using a third party service provider. Users can communicate business documents such as purchase orders, price quotes, shipping notices or even payment orders, electronic funds transfer to customers and suppliers. The format in EDI is governed by a set of standards. Essentially an EDI system comprises four basic elements as shown in figure 2.1. These are:

2.1.1 Application to Application Process

EDI is a direct application to application communication as opposed to computer to computer communication. At the simplest level, one (the sender) application generates information which is processed by a second (the recipi-

ent) application. An important distinguishing characteristic of EDI systems is that the two applications are geographically distant. The EDI system requires the data to be in a highly structured format according to the EDI standards.

2.1.2 Standards

The use of structured, formatted messages based upon internationally agreed standards are necessary in an EDI because they enable messages to be translated, interpreted and checked for compliance to a standard set of rules. It requires a set of procedures (and protocols) for converting the information from the native format generated by the sender application into a previously agreed standardized format (e.g. ANSI X12, EDIFACT, etc.) for interchange. The recipient application has access to a corresponding set of translation services which convert the information from the standardized format to the required native format. Often they are processed in batches, or they can be handled directly in real time. This allows companies to enquire directly on their trading partner's system (where authorized) for information such as price, availability, order status etc.

2.1.3 Translation Software

The EDI translational software links the application and the communications software and makes the EDI process functional. This software allows for the translation of data from a company's internal format to the industry specific format. EDI translation software has two primary functions. For outgoing data, the software reformats the electronic data into the public or industry standard used by the receiving partner. For incoming data, the software reformats the EDI data into the format required by the internal application

and performs edit checks. EDI translation software typically consists of a communication link and an application interface. The *communications link* is responsible for sending and receiving teleprocessing commands along the network that connects the trading partners and the third party service providers. The *application interface* controls the sending and receiving of EDI messages, or transactions, to and from the document database.

2.1.4 Communication Networks

The telecommunications hardware and software are the components that create the link between the trading partners and provide the partners with the capability to send and receive EDI transaction sets. The use of electronic mailboxes for "store and collect/store and forward" transmission/delivery of documents is provided by the third party network service provider. Thus it requires a set of procedures (and protocols) for packaging the information generated by the previous (information format conversion) phase into the format required by the communication network service used to transport the information between the communicating applications. Telecommunication software controls the actual transmission of EDI messages. Features of this software can include automatic dialing, management and maintenance of trading partners addresses and activity logging.

The aims of EDI will only be realized if the EDI systems incorporate appropriate communication mechanisms. The requirements for such communication systems include:

- The communication should be independent of machine, media and the end system allowing trading partners to operate within their own computing strategies without being restricted by the EDI systems;

- The communication system does not affect existing data processing applications;
- The EDI messages should not be affected by the use of a particular communications protocol;
- The communication must handle messages of the format used by EDI, or that of a general purpose communication system which can handle any format of the message being used;
- The communication must provide services that are required by the processes that are inter-working to provide EDI. These services include definitions of what happens if the EDI message cannot be delivered.

Thus the term Electronic Data Interchange does not refer to:

- *Electronic mail* : Like Electronic Data Interchange, electronic mail also moves business data electronically, but generally uses a free rather than a structured format. Since the sender may choose any format, it is difficult to design an application program that would directly accept electronic mail input without significant manual editing.
- *Facsimile Transmission* : Facsimile transmission represents the transfer of totally unstructured data. Data in almost any format, from photographs to purchase orders, may be sent by this means. In facsimile transmission, a digitized image is formed of the message and the image is transmitted to the receiver. The receiver of the facsimile transmission would not be able to enter the image directly into a business application without manually keying in the printed image or at best editing the character file by some means.

- *File Transfer* : This application also makes little use of standard formats which need not have any connection with applications at either end of transmission.

In the next section the benefits offered by the use of Electronic Data Interchange in an organization are examined.

2.2 Benefits of EDI

The use of EDI is increasing on a global scale. The efficiency and cost-saving aspects of EDI form a strong basis for its growing popularity in the world of electronic transactions. Major organizations have been at the forefront of EDI, and smaller entities are aligning themselves along the "paperless" path of business transaction and communication. Although the case for an EDI differ between companies, several key reasons such as improved customer service; reduced operating costs and responsiveness to market demands continually re-occur. The key benefits which result from the employment of EDI in an organization include :–

2.2.1 Improved Productivity

There is improved productivity using EDI with the reduction in paper flow and support for just-in-time inventories. The benefits normally associated with the reduction in paper work in an EDI environment include personnel savings, better data quality and improved customer service. In addition, savings may be attributed to the reduction or elimination of data entry requirements. The electronic transfer of business documents improves data quality by minimizing potential misinterpretation resulting in an error in data quality. EDI improves

customer service by compressing the inherent time delays in the value added chain, thus greatly reducing the possibility of lost or missing information.

2.2.2 Competitive Advantage

In a highly competitive market, the ability to offer significant cuts in product delivery time may be the difference between winning and losing a contract. This is particularly relevant to international trade, where the movement of paperwork can lag behind the associated movement of goods, resulting in goods being tied up in port waiting for clearance. The net effect is increased cost to the carrier, which filters through into increased cost to the customer.

2.2.3 Reduced Financial Exposure

With the use of EDI, the financial exposure risks are reduced thereby making cash management more efficient. Commercial risks may be contained by developing fewer but stronger supplier relationships. When the barriers to inter-organizational communication are greatly reduced, the quality of the relationship should improve. EDI enables suppliers to send accurate and timely invoices. Customers report vast improvements in matching invoices with purchase orders and deliveries, and a reduction in the number of errors and queries. The net result is that a high proportion of invoices are on time.

2.3 Who Should Use EDI ?

The use of EDI is steadily growing across all industries. One of the driving forces behind the implementation of EDI is the external pressure from customers. Companies fear losing their business advantage if they do not implement EDI in their organization. The potential organizations that may require

to implement EDI include those who

- Handle large volumes of repetitive standard transactions which is an important factor in transportation and groceries industries.
- Operate on a very tight margin.
- Face stiff competition, requiring significant productivity improvements.
- Operate on a time-sensitive environment.
- Have received requests to convert to EDI from trading partners.

2.4 Implementing EDI

Pugsley [44] has defined six steps to successfully implement EDI technology in an organization:

- *Complete understanding of EDI* : The depth of knowledge a company acquires on EDI depends on the internal efforts spent. If no external consultants are hired then the level of knowledge should be high. One method to gain knowledge is to join one of the groups developing standards. (e.g. EDI Council of Australia)
- *Agreed on standards with business partners* : After finding a suitable business partner, agreements should be made concerning standards, transactions to be exchanged, message syntax, file transfer protocol etc.
- *Modifying existing systems* : The host computer applications should be modified so that EDI information is incorporated or integrated directly into the applications. Good EDI software should provide an application interface to many different applications.

- *Translate data* : Various translation modules are required to translate transactions into EDI messages according to the EDI standard being used. The translation is required of the data into the EDI format as well as translation of data from an EDI package into a format compatible with the in-house application.

- *Prepare communications* : A network connection to various trading partners is required via either a Value Added Network (VAN) or direct connection.

- *Management and audit of the whole process* : Consistent management and auditing of the entire process must be established and maintained. The tasks include archiving transactions, inspecting error logs and ensuring security of the system.

Direct computer-to-computer communications with a trading partner requires that both firms use similar communication protocols; have the same transmission speed; have telephone lines available at the same time and have compatible computer hardware. If these conditions are not met, communication becomes difficult, if not impossible. A Value- Added Network (VAN) can solve these problems by providing services that enhance the basic telecommunication network.

2.5 Value Added Network (VAN)

A VAN, at the simplest level, provides point-to-point packet switching. At a more advanced level it may also offer protocol conversion to support a wide range of different equipment. A comprehensive VAN is likely to have the following general components – basic network, generic services, transaction relay,

application enabling, information databases and network management. It will also provide a two-way link that enables users to rapidly exchange records or specific fields of an EDI message rather than the whole message, but it is more commonly used as a store and forward service that employs electronic mailboxes to which messages are sent. By using VAN services, a company can trade electronically with many trading partners and yet only need to meet one set of EDI communications requirements - those determined by the user's chosen VAN.

The commonly available VAN service providers are GEIS EDI exchanges, IBM's Information Exchange EDI Service, British Telecom's EDI*Net service.

2.5.1 Benefits of VAN

Generally trading partners do not operate in the same computer environment nor use the same data format. VANs put order into this EDI world by performing conversions between different trading partner environments, thus enabling many trading partners to work as a single user community. The additional benefits obtained in using a VAN are:

- A direct communication link to any trading partner
- VAN service providers' experience and knowledge of the existing EDI standards and evolving EDI technologies;
- A VAN's ability to support multiple data format standards;
- VAN mailbox services, a store and forward system of messaging;
- 24 hour services; and

- VAN's ability to provide tracking and control information, with which users audit document and message transmission between partners.

2.6 Existing Third Party Service Providers

There are number of Third Party Service Providers available which offer value added services to the customers. The basic security service provided is through the use of passwords.

In Trada-Net, there is high physical security. Access to the system is through passwords which are changed daily. However, the messages can only be sent through the service after prior agreement of both the trading partners for exchange of particular data type. There are audit trails for the complete transactions and the third party also offers facility of doing trading defined in a closed user group.

The world's largest EDI third party service provider is GEIS. It provides physical safeguards to the incoming lines. In addition, distribution to different lines is done via two levels of random access devices before the messages are routed out to the leased lines (i.e. message bit stream is also split). It also provides added security functions such as an option for a secondary password and requirement of session code when transferring funds.

2.7 Summary

This chapter outlined the basic concepts of an EDI, its advantages and the benefits to improving business relationships. Since EDI involves paperless

transactions, there is greater need to prove that the transactions are authentic and they must be protected against misuse and fraud. In the next chapter the security threats that are inherent in an EDI system are discussed.

Chapter 3

Security Issues in EDI

> A threat is a circumstance, condition or event with the potential to cause harm to personnel and/or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste and abuse. [25].

Due to the basic nature of paperless transactions in Electronic Data Interchange (EDI), the security of an EDI system should be studied in greater detail. This chapter addresses the security threats inherent in the present day EDI systems such as password guessing attacks, cross-vulnerability, multiplicity of standards along with the threats encountered in distributed systems.

3.1 Basic Concepts

As mentioned in the previous chapter, EDI is becoming an accepted business technology for participating in today's global market. However, this technology cannot be implemented in a risk free environment. Users must be assured that full consideration has been given to the security issues inherent in the use of computers and telecommunications in accomplishing traditional paper-

based activities. Such processes have been targets of fraud and other criminal threats. Most companies believe that the current EDI agreements and third party service providers offer adequate security against fraud and errors in EDI transactions. This is far from true. There is a definite need to upgrade the existing security as the complexity of EDI communities grow [18].

The concept of data security developed long before computers. For example, cheques are usually written with the background patterns to detect manual alteration, while watermarks and other hidden image graphics are used to deter the use of photocopies. The difference between security for paper cheques and security for electronic transactions lies in the ways in which fraud can occur. In electronic transactions fraud can occur through access to unprotected data terminals or electronic files or through interception of data as it is being transmitted. There are several transmission link types which can be chosen by a network – wired cables, terrestrial microwave, communication satellites and optical fibers. Different tapping risks exist and different methods are available for tapping of each type of link [28]. Commercial network suppliers such as INS, ISTEL and IBM have built exhaustive security systems into their networks to deter unauthorized entry into the system, although this does not guard against the possibility of detectionless methods of tapping such as interception of microwave transmission or wiretapping.

The level of security sought must be consistent with factors such as: perceived threats to the system; perceived value of the information contained in the system and the internal and legal requirements (i.e. audit trails) of an organization. The implemented countermeasures must be balanced between the perceived threats, economics, ease of use and maintenance of the system.

Keeping these factors in view, the following security issues need to be countered to ensure the smooth and secure operation of an EDI system.

3.2 EDI Security Issues

For the EDI to be widely accepted in commercial trading, users must be assured that the electronic system provides them with the equivalent protection against mistakes, misinterpretation and fraudulent activities that is offered by the paper and signature system to which they are accustomed. The following security issues related to EDI are discussed in view of the security offered in the present day systems.

3.2.1 Password Guessing Attacks

Most of the present day systems rely on passwords to gain access but, passwords are easy to guess and this makes the system vulnerable to password guessing attacks. Users are very poor in choosing good passwords. An intruder can capture a quantity X that is derived from a password in a known way. Then the intruder can use an arbitrate amount of computing power to guess passwords, convert them in a known way and see if X is produced. The best source of selecting such passwords is the dictionary and hence it is also called as *dictionary attack.* e.g. In Kerberos Authentication System [29, 34], when the user requests the ticket granting ticket ($T_{c,tgs}$), the answer is returned encrypted with K_c, a key derived by a publicly-known algorithm from the user's password. A guess at the user's password can be confirmed by calculating K_c and using it to decrypt the recorded answer. An intruder, who has recorded many such login dialogs, has good odds of finding several new

passwords.

3.2.2 Cross Vulnerability

Generally EDI systems work on a point to point basis or have a limited number of trading partners. The security and control features incorporated in the system are as strong as the weakest link in the EDI chain. A potential exposure or cross-vulnerability due to technical limitation in one EDI system can compromise the integrity of the other dependent EDI systems. Cross-vulnerabilities exist between systems that rely on common values for user identification and authentication, such as IDs and passwords.

3.2.3 Multiple Standards

Trading partners usually work on a variety of standards such as UN/EDIFACT, ANSI X12, ODETTE etc. Problems arise when the two trading partners adhere to different standards. The security features offered in a particular standard may not be comparable to the other standard.

3.2.4 Authentication

The extensive use of open networks and distributed systems poses serious threats to the security of end-to-end communications and network components themselves. A necessary foundation for securing a network is the ability to reliably authenticate communication partners and other network entities. Authentication is the most important of the security services, because all other security services depend upon it. Authentication relates to a scenario where a claimant has presented a principal's identity and claims to be that principal. Authentication enables a verifier to verify the identity of the principal.

3.2.5 Non-Repudiation

In EDI, non-repudiation services provide a communication user with protection against another user who later denies that some communication exchange took place. While these services do not prevent a user from repudiating another user's claim that something occurred, they provide evidence to resolve any such disagreement. In general, the evidence must be proved convincingly to the third party arbitrator. In data networking environments, repudiation scenarios can be separated into two distinct cases:

- *Repudiation of origin* : There is disagreement as to whether a particular party originated a particular data item.
- *Repudiation of delivery* : There is disagreement as to whether a particular item was delivered to a receiving party.

3.2.6 Disclosure of Information

With the introduction and use of EDI, additional security risks arise apart from those which exist for the conventional electronic information systems. The computers of a trading partner can initiate transactions inside another partner's accounting systems which are processed in a totally automatic environment. By its very nature, EDI requires that the system be continuously open to receive incoming transactions. This means that the system and the associated data are exposed continuously to attack and possible compromise. An EDI trading agreement is done for the exchange of data among geographically dispersed participants. Consequently this mechanism is exposed to all threats to which the telecommunication system is subjected. Therefore all data protection requirements for a distributed telecommunication process are

applicable to an EDI trading agreements.

3.2.7 Lack of Hard Copy

With EDI, the information concerning predetermined subject matter that could be conveyed on paper is transferred as a set of electronic messages in standardized formats. The information may remain in electronic form and may never be printed. The lack of hard copy records and manual signatures creates new risks that must be carefully considered in any EDI implementation. As a result, original hard-copy evidence of obligation or commitment by the trading partners may not be available. Instead, electronic records must be used. Specific activities must be undertaken to assure that EDI messages, such as electronic records, are authentic, properly authorized and completely and accurately retained with audit trails for purposes of accountability.

3.2.8 Other Issues

In order to accommodate the increased need of the user community, as the complexity of an EDI system grows, the security services also need to be upgraded. In addition, there are various network security threats that need to be countered in an EDI system. They include eavesdropping, denial of service, packet replay and packet modification.

Eavesdropping

Eavesdropping allows an intruder to make a complete transcript of network activity. As a result, the intruder can obtain sensitive information, such as passwords, data, and procedures for performing functions. An intruder can

gain information by wire tapping, eavesdropping by radio or eavesdropping via auxiliary ports on terminals. In today's competitive world, disclosure of information about a company may prove fatal for the future of the company.

Denial of Service

Multi-user, multi-tasking operating systems are subject to denial of service attacks where one user can render the system unusable for legitimate users by damaging or destroying resources so that they cannot be used. They may be caused accidentally or deliberately. It will help to prevent intentional denial of service attacks if precautions are taken to prevent unintentional denial of service attacks.

Systems on a network are vulnerable to overload and destructive attacks as well as other types of intentional or unintentional denial of service attacks. Three common forms of network denial of service attacks are service overloading, message flooding and signal grounding. In service overloading, the intruder generates spurious messages to increase the traffic in the network thereby degrading the service to the user. In message flooding, the intruder generates confusing routing messages or simply flood the network with enough garbage data to saturate the links. This may make the network inoperative. An active intruder can disrupt the service or ground the signals by intercepting or destroying messages for a particular user. It is important for system administrators to protect against denial of service threats in an EDI system without denying access to legitimate users.

Packet Replay

Packet replay refers to the recording and the re-transmission of message packets in the network. Packet replay is a significant threat for an EDI System because an intruder could replay legitimate authentication sequence messages to gain access to an EDI system. Packet replay is frequently undetectable, but can be prevented by using packet time-stamping and packet sequence counting.

Packet Modification

Packet modification is a significant integrity threat which involves one system intercepting and modifying a packet destined for another system. In many cases, packet information may not only be modified, but may also be destroyed.

3.3 Risk Analysis

To counter the above mentioned threats effectively, a risk analysis should be performed by the systems staff at the initiation of an EDI project. The risk analysis should focus on the these potential risks:

- Authorized personnel can initiate unauthorized or erroneous transactions that could result in excessive costs, fraud, embarrassment, or legal exposure.
- Unauthorized users can gain access to EDI applications and initiate unauthorized transactions or destroy data.
- Data can be lost, inaccurately transmitted, or altered during transmission.
- The EDI application does not meet business objectives or satisfy either user or control requirements.

- Adequate audit trails are not maintained, impairing the organization's ability to evaluate controls or potentially exposing it to legal liability.
- As a result of control weaknesses, the organization is exposed to the environment of trading partners.
- The trading partner agreement does not adequately address liabilities for protection of proprietary data, the required components to constitute a binding agreement or other necessary clauses.
- Formal contracts with third party EDI service providers do not adequately address security, system reliability and availability, or responsibilities.

3.4 Summary

This chapter described the security threats in an EDI system. In chapter 5,6 and 7, the *Direct Store Delivery System*, a model of an EDI system which provides the security services for user identification, global authentication, user authorization and non-repudiation services is described.

Chapter 4

Standards for Secure Message Handling

This chapter describes the X.400, X.500 standards for secure message handling. In particular, those security services offered in these standards which can be used on a global basis in a networked environment are examined.

4.1 X.400 Overview

The X.400 Message Handling System is a form of store and forward type of message transfer, including transfer of electronic business data interchange and voice messaging. The standards provide security services for end-to-end security. A more detailed description is available in the literature [15, 16, 18]. In this section, three main aspects of the MHS are described. the functional model, the message structure and delivery reporting from the security point of view.

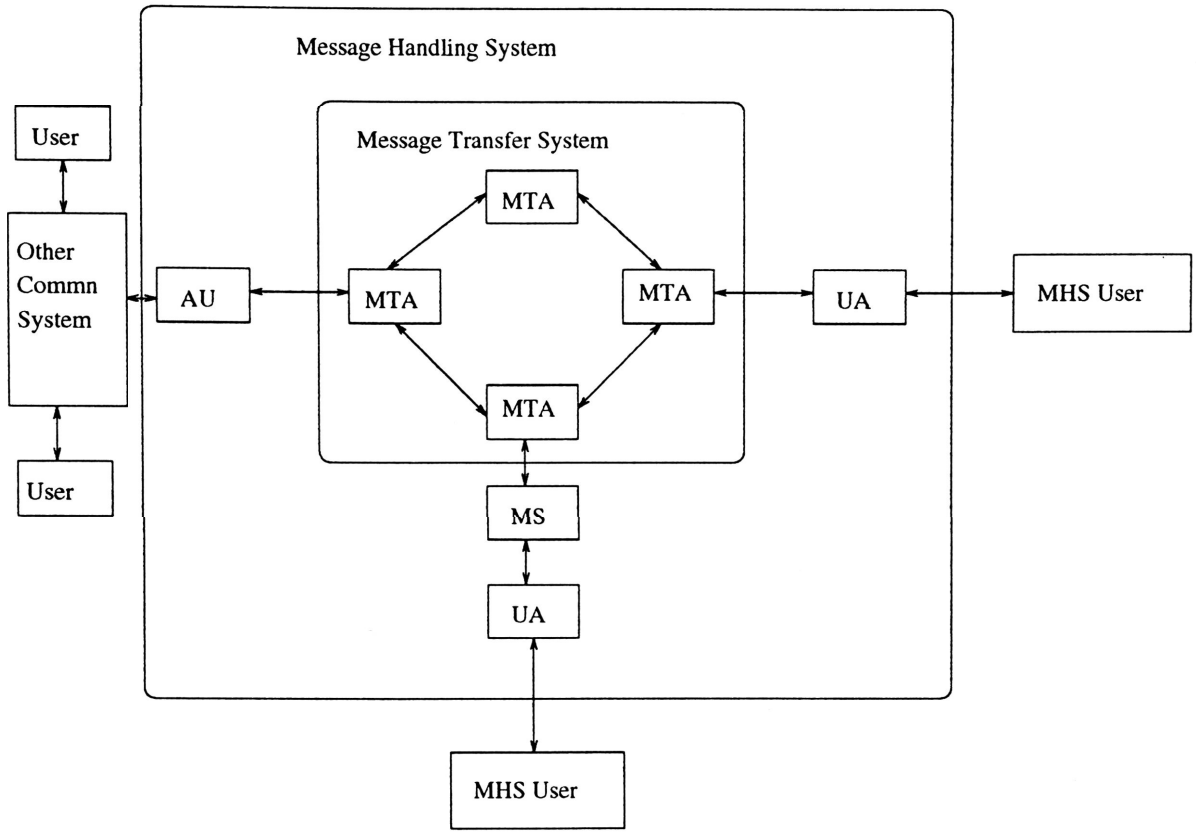


Figure 4.1: Message Handling System

4.1.1 Functional Model

A functional model [25] is shown in the figure 4.1. The MHS is a collection of MTAs (Message Transfer Agents), MSs (Message Stores), UAs (User Agents) and AUs (Access Units). MTAs perform the store-and-forward message transfer function. MSs provide storage for messages. UAs enable users to access the MHS and AUs provide links to other communication systems. MTAs comprise of MTS (Message Transfer System), the principal component of the MHS. A message is submitted to an MTA by an originating UA, MS or AU, transferred to the recipient MTA(s) and delivered to one or more recipient UAs, MSs or AUs. If the message is addressed to multiple recipients, the appropriate MTAs perform any splitting (i.e. replicating) of the message needed for delivery to each recipient.

Messages are transferred between MTAs on a cooperating store-and-forward basis. Since no end-to-end association is required, the MTA serving the message recipient need not be active when the message leaves the originating MTA. The message may be stored at an intermediate MTA until the recipient MTA becomes operational.

MTAs transfer messages whose content may be encoded in any format. MTAs neither examine nor modify the content of messages except when they are performing conversion. Conversion increases the effectiveness of the MHS by allowing users to submit messages in one encoded format (e.g. telex) and have them delivered in another encoded format. A UA can register with the MTA the encoded information types that may be delivered, and request the MTA to perform any required conversions.

The UA is the MHS component that enables a user to access the MHS, for both the origination and reception of messages. When submitting messages, the UA supplies to an MTA, either directly or indirectly via an MS, the message content, the address(es) of the message recipient(s) and the MTS services being requested. The message content is the information that the originator wants transferred to the message recipient(s). The addresses and service request data are used by the MTS to deliver the message. When receiving messages, the UA may accept delivery of messages directly from an MTA, or it may employ an MS to accept delivery of messages and retrieve them from the MHS at a later time.

The MS is an optional MHS component that acts as an intermediary be-

tween a UA and MTA. The MS often resides with the MTA serving it. The primary purpose of the MS is to provide a repository for the delivery of messages. The UA can retrieve messages from this repository. By using an MS to accept delivery of messages, a UA is not required to be constantly available. This is especially useful for UA applications implemented on a PC. The MS may also submit and forward messages on behalf of the UA, and notify the UA at the time of message delivery.

The AU is the MHS component that provides a gateway between the MHS and another communications system. Another AU, the PDAU (Physical Delivery Access Unit) enables MHS users to send messages to users residing on a physical delivery system such as an EDI mailbox.

4.1.2 Message Structure

The message structure consists of a message envelope and a message content. The envelope represents the information required by the MTS to deliver the message, such as the address of the recipient and any special handling instructions. Many X.400 security parameters are transferred on the message envelope. The message content represents the information that the originator wants conveyed to the message recipient.

4.1.3 Delivery Reporting

The basic X.400 messaging service provides notification of message non-delivery. When a message cannot be delivered to a recipient, a non-delivery report is generated and returned to the originator. The content of the non-delivery report contains the status information about the subject message. The MTA

also provides notification of delivery as an optional service. If the message originator requests acknowledgment of successful delivery, a delivery report is returned to the originator by the recipient's MTA upon delivery of the subject message.

4.2 Security Related Data Structures

The security label and the token are used to convey security related information between communicating parties. This section defines only the principal attributes comprising the structures.

4.2.1 Security Label

A security label is a collection of attributes associated with an MHS message or entity which permits its classification in terms of a security level. The security label attributes include:

A security policy identifier which identifies the security policy with which the security label is associated,

A printable privacy mark which identifies the level of privacy to be afforded in a message or report,

A security classification which classifies a message or report for security purposes,

A set of security categories which restricts the context of the privacy mark, the security classification, or both. The categories are application-defined, and may include codewords to the privacy mark or security classification.

Security labels may be transferred in MHS messages and reports, conveyed during the association establishment between the two entities (e.g. A UA may

transfer security labels when connecting to its MTA), or registered with MHS entities (e.g. an MTA may maintain a registry of security labels for its users).

4.2.2 Token

The token is a signed data structure used to convey security-related information from an originator to a single recipient. It consists of a series of data fields with the digital signature appended. The general form of a token is:

$$\mathrm{A}\{sgnAlg,\ t^A,\ \mathrm{B},\ sgnData,\ encAlg,\ B_p[encData]\ \}$$

where A is the name of the originator of the token, *sgnAlg* identifies the algorithm used by the originator to compute the signature, t^A is a time stamp, B is the name of the intended recipient, $B_p[encData]$ is the data *encData* encrypted under the public key of B i.e. B_p, *encAlg* identifies the asymmetric algorithm used to perform this encryption, and *sgnData* and *encData* are collections of security related parameters. The contents of the *sgnData* and *encData* depend on the security services being provided. The attributes comprising the token include:

- the name of the recipient
- the date and time the token was generated
- a collection of additional fields that is signed (signed-data):
  - a content confidentiality algorithm identifier,
  - a content interity check,
  - a message security label,
  - a request for proof of delivery,
  - a message sequence number,

- a nonce

- a collection of data fields that is encrypted (encrypted-data):
  - a symmetric key used to encrypt the content,
  - a symmetric key used to compute a content integrity check,
  - a content integrity check,
  - a message security label,
  - a message sequence number.

The attributes of the token are protected by the digital signature of the originator. The token provides three forms of cryptographic protection. First, it ensures that only the recipient can view the plaintext information in the encrypted-data. Second, it ensures that the token has not been modified. Third, it authenticates the identity of the token originator.

4.3 X.400 Security Limitations

The basic security services provided by the X.400 standards include: *message security labeling, secure access management, origin authentication, data integrity, data confidentiality, non-repudiation* and *security management.*

One security limitation is that the data in the token is encrypted before it is signed. This is considered to be a poor practice because the recipient can authenticate the encrypted data, not the plaintext data. In a worst case scenario, a malicious party can intercept a message, and create a new message keeping the encrypted content of the original message, but generating a new message token. The new token would be signed by the malicious party. Under these

circumstances, the message recipient could could be fooled into believing that the malicious party originated the message. This can be avoided depending on how the security services are implemented. For instance, defining a token so that the encryption is performed after the signature is calculated, removes the limitations but at the cost of some increase in processing.

A second limitation pertains to the MS (Message Store). An MS can accept the delivery of messages on behalf of a UA. If a message originator requests *proof of delivery* for a message whose content is encrypted, and the message is delivered to an MS, the MS would require access to the encryption key to provide the service. This would involve providing the MS with the recipient's private key to decrypt the message and perform verification, or providing a shared key between the recipient and the originator. Neither case is desirable from a security standpoint. This is one scenario where a recipient (i.e. the Message Store) might ignore the originator's request for *proof of delivery.*

A final limitation pertains to the MTS services which access the message content or message recipient. An MTA may perform conversion on incoming messages. Any type of conversion invalidates integrity checks. Also, if the content is encrypted, the conversion cannot be performed without the MTA first decrypting the content. To decrypt the content, the MTA would access the encryption key, which is not desirable from the security point of view. Similar problems result from services that modify the message recipient, such as MTA expanding a distribution list or redirecting a message. If an MTA performs such a service on a message where the recipient's public key is used as input to some security service (e.g. to encrypt the encrypted-data of a token), the security service must be calculated using the public key of the new recipient.

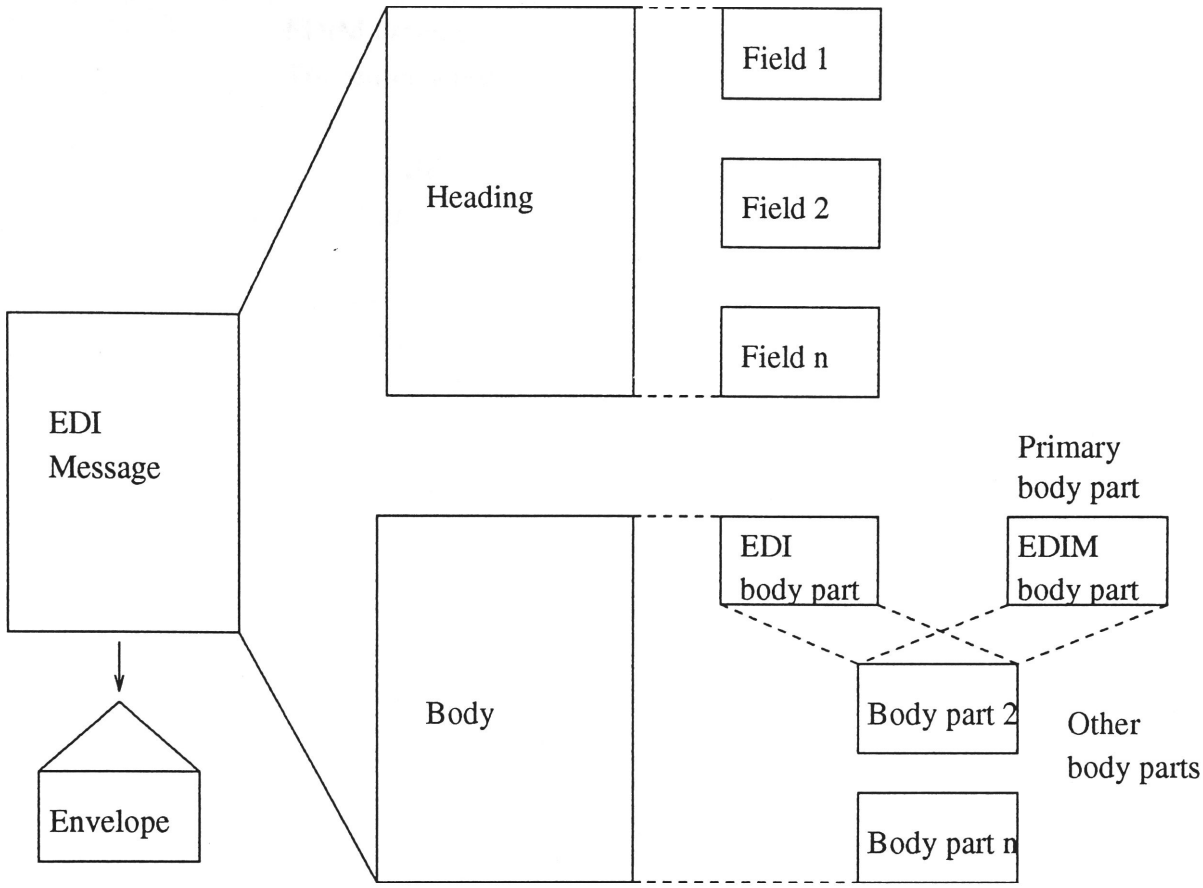


Figure 4.2: EDI Message Structure

The communication of EDI messages require that the messages are in structured format before they are transmitted on a network. To facilitate the transmission of structured messages in a message handling system, X.435 or Pedi standard was developed.

4.4 X.435

EDI interchanges can be conveyed in many ways – directly over a telephone line or encapsulated in a file transfer.

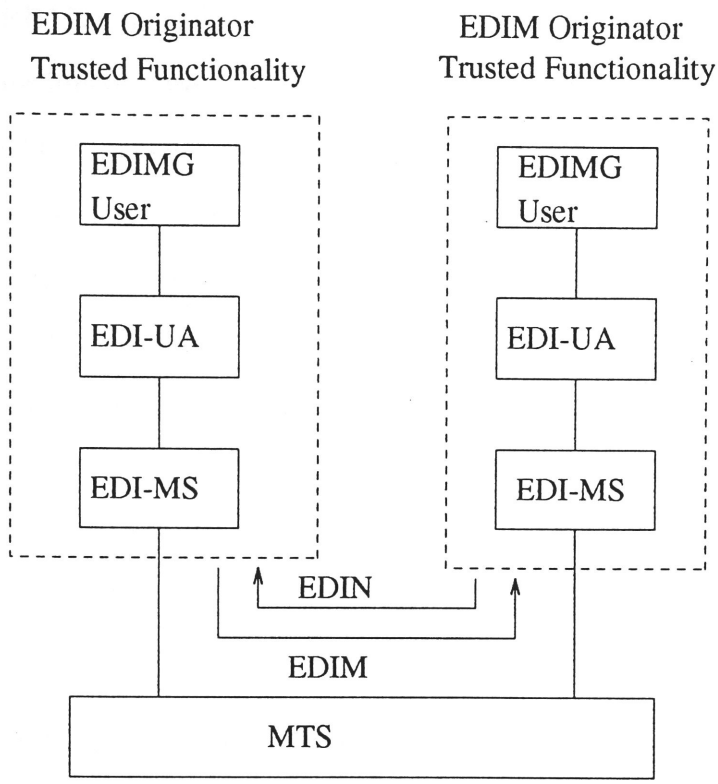


Figure 4.3: X.435 Security

The basic concept in X.435 standard is that there are special EDI messages (EDIMs) consisting of a heading and a body part as shown in the figure 4.2 Typically a body part could be an EDIFACT interchange or an ANSI X.12 EDI interchange. The heading contains many fields concerned with identifying the message and specifying how it is to be handled. An EDI message can be broken down into several components:

- Data Elements – the smallest indivisible piece of data which is equivalent to words in the spoken language;
- Segments – a set or group of related data elements;
- Messages – a set or group of segments in the order specified by the standard. Each message specifies a specific transaction.

Additionally, EDI Notifications (EDINs) exist, specifically to address the problem of confirmation of receipt at the application level (i.e. by the receiving EDI application) as opposed to simply confirmation of delivery. In figure 4.3, there is a special EDI-UA together in a trusted environment that accesses the underlying MTS, with added EDI-MS. EDINs are special messages linked to the original subject EDIM by appropriate cross references. They contain a series of common fields followed by positive, negative or forwarded fields, depending on the nature of EDINs. EDIMs and EDINs introduce new security elements of services, essentially to guarantee the genuineness of EDIN, as valid confirmation of EDIMs.

4.5 X.500 Directory Services

The objective of the X.500 Directory is to provide a logical global database for public and private directory services. The Directory is a collection of distributed open systems that cooperate to hold a logical database of information about a set of objects in the real world. The users of the Directory can read or modify the information, or parts of it, subject to permission being given. The access to the Directory is interactive – supporting both browsing and automatic lookup. The application process employs user friendly naming schemes to achieve this.

A global directory requires co-operation between a large number of network operators and service providers, each of which administers a range of names and addresses and maintains its own separate database. There are three kinds of information held in a directory:

- *User information* that is intended for use primarily by the people and

systems that access the Directory to obtain data such as electronic mail address, phone numbers, network address and public key identity certificates.

- *Operational information* that is intended for use primarily by the Directory system itself. Examples of such systems include access controls and internal consistency requirements that the Directory must maintain.

- *Server information* that is used by each server to identify the location and contents of the other servers.

4.5.1 Functional Organization of Directory

The X.500 Directory Standard identifies two major functional components for the Directory. These are the Directory User Agent (DUA) and the Directory System Agent (DSA). The DUA represents a user of the Directory and provides access to the DSAs that process the actual Directory requests. The Directory information may be distributed amongst a set of co-operating DSAs to provide an integrated service called a Distributed Directory. A DSA may also operate as a free standing single database, referred to as a Centralized Directory. The overview of the distributed directory is shown in figure 4.4 The information entries contained in the Directory are referred to as the Directory Information Base (DIB) which is structured to form a Directory Information Tree (DIT). The protocols that take place within a directory are Directory Access Protocol (DAP) which define the exchange of requests and outcomes between DUA and DSA; and Directory System Protocol (DSP) which defines the exchange of requests and outcomes between two DSAs.

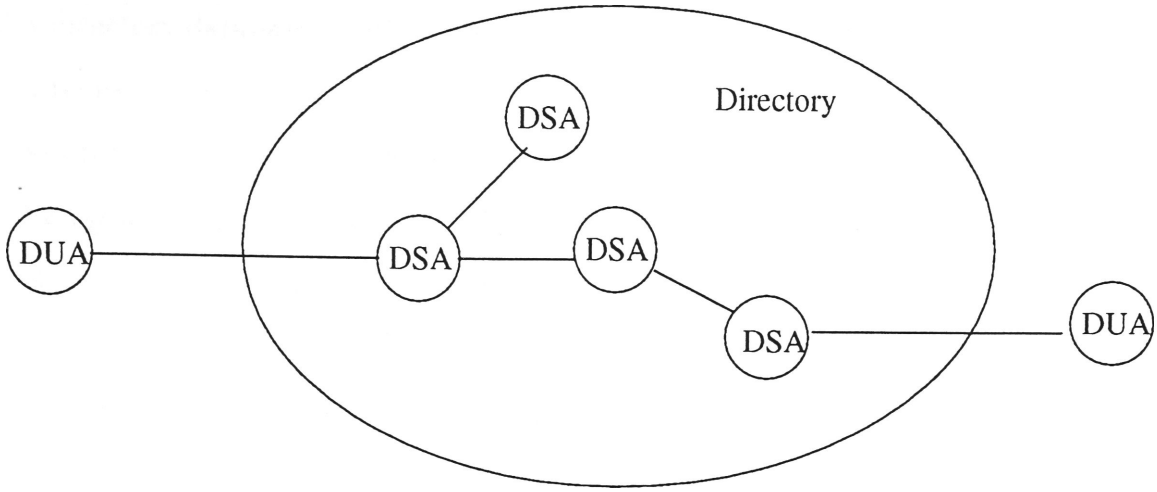


Figure 4.4: Distributed Directory

4.5.2 X.509 Directory Authentication Framework

The recommendations define a framework for the provision of authentication services by the Directory to its users. The recommendations provide two complementary goals:

- distribution of trusted keys and enforcement of access controls to information based on the rights of the requester.
- confidence held in the information held in the Directory provided to identify that user.

Authentication can only be provided within the context of a defined security policy. The recommendations provide two types of authentication – simple authentication based on password as a verification of claimed identity and strong authentication employing credentials formed using cryptographic techniques which will be described in chapter 7.

The Directory recommendations are based on public key cryptosystems. It is a major advantage of such systems that the user certificates may be held in

a directory database as attributes and may be freely communicated within the directory systems and obtained by users of the Directory in the same manner as other directory information. The user certificates are assumed to be formed by *offline* means and placed in the Directory by its creator (Certification Authority). When a CA issues a certificate to a user, the certificate binds the name and the public component of the user. The general structure of the certificate using the Abstract Syntax Notation (ASN) is:

```
Certificate := SIGNED { SEQUENCE {
        Version                 [0] Version DEFAULT v1,
        SerialNumber            CertificateSerialNumber,
        Signature               AlgorithmIdentifier,
        Issuer                  Name,
        Validity                Validity,
        Subject                 Name,
        SubjectPublickeyInfo    SubjectPublicKeyInfo,
        IssuerUniqueIdentifier  [1] IMPLICIT UniqueIdentifier OPTIONAL,
                                - - if present, version must be v2
        SubjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL
                                - - if present, version must be v2 - - } }
```

Before users can mutually authenticate, the Directory will supply complete certification and return certification paths.

4.6 Summary

The MHS (X.400) standards include very comprehensive security facilities. The basic end-to-end services are provided without having to trust the under-

lying MTS. The message path services contribute to secure communications throughout the MHS environment, placing requirements on functional components of all types. Transfer of EDI transactions over the MHS backbone employs a special MHS content type. Security functions can also be provided within the EDI content, using features in the EDI format.

The Directory is an important open-system network application which can play a valuable role in supporting the information retrieval needs of other applications. The Directory is also significant to network security because of the role it can play as a distributor of public key certificates for use by any network application.

In the next chapter, we use these standards in the proposed model to provide the security services.

Chapter 5

Direct Store Delivery System

This chapter describes the proposed model of the Direct Store Delivery System. In the model, the transactions are carried out using a trusted third party service provider or Value Added Network Service provider. Basic functions such as user registration, notary services, key management facilities, audit trails and secure gateways are provided by the third party service provider. In the proposed model, the X.500 standards were used based on the Directory Services for resolving address issues and mutual authentication based on principal global identity. The transactions of the EDI messages are carried out using the UN/EDIFACT standard in a message handling system environment.

5.1 The System Model

The Direct Store Delivery System [10] model is based on the concept of JIT inventory management. In business, JIT inventory management is gaining widespread acceptance especially amongst retailers. It focuses on the reduction of the inventories of the companies involved and the audit of their production. Essentially, it optimizes supplier and customer relationships. Production and

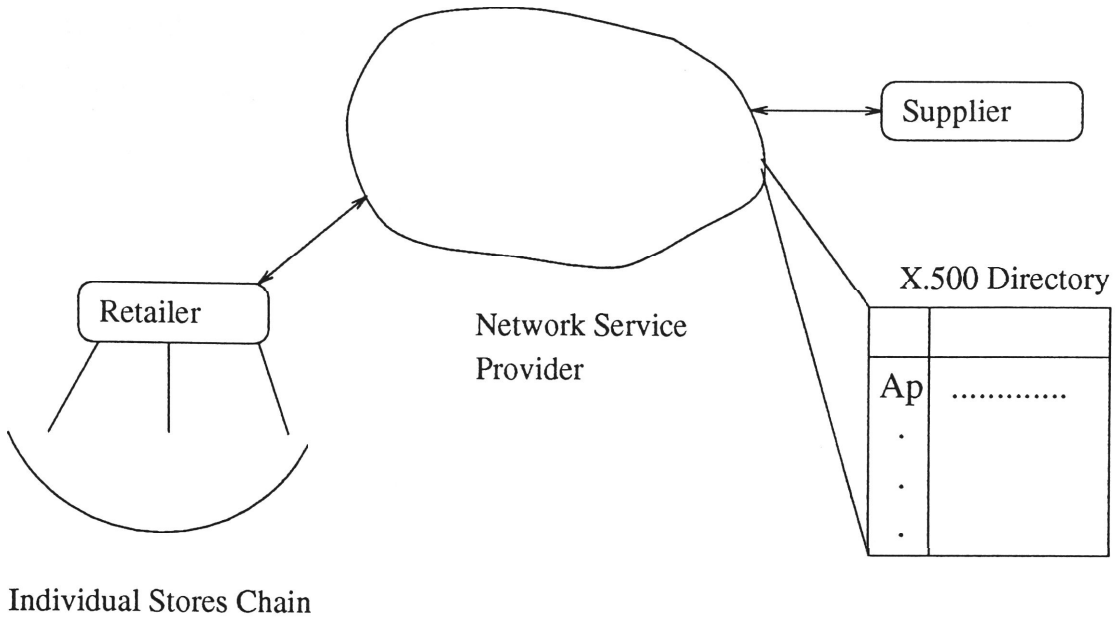


Figure 5.1: Direct Store Delivery System

inventory costs are decreased as the required level of stock is reduced. EDI facilitates the adoption of these JIT techniques by providing timely and accurate information which is required on a daily basis, whilst promoting the trust and commitment required on a long term basis.

The Direct Store Delivery System is a chain of stores where ordering and deliveries are carried out centrally. The chain handles the distribution to the individual stores as shown in figure 5.1. It uses EDI to place bulk order on the suppliers nominating the quantity needed and the expected time of delivery. Thus, the retailers continue to get the benefit of centralized ordering and as a consequence reduces inventory and saves on warehouse and material handling costs. The merchandise can be ordered faster and a given item is never out of stock. The use of Electronic Data Interchange results in error reduction in entering data, reduces paperwork and improves cash flow thus resulting in an efficient trading cycle.

To be able to communicate efficiently with trading partners, the X.500 standards for user friendly addressing is used. Trading can be carried out on a global basis since the users have unique names and are identified on the basis of principal global identity. In accordance to the X.509 Directory Authentication Framework, the certificates contain public keys of the trading partners which can be freely communicated in a distributed environment.

The system is modeled in an EDI Messaging System as shown in figure 5.2. The EDI service provides a user with features to assist in communicating with other service users. The EDIMS model comprises of an EDI User Agent, EDI Message Store and Access Units, all of which are supported by the Message Handling System. The UAs in the EDIMS comprise of a specific class of co-operating UAs. The Physical Delivery Access Unit allows EDI Users to send messages to users outside the EDIMS who have no access to the MHS. The EDI class of UAs create messages containing contents specific to the EDI Messaging Service. The EDI message is conveyed in an envelope when being transferred through the MTS. The whole transaction process can be divided into the following independent processes.

5.1.1 Sending EDI Messages

Before the actual messages are sent, they need to be processed including the conversion of the in-house application into a structured EDI message. The initiation process creates the addressing/envelope information necessary to route the EDI message through X.400 Message Handling System. The EDI initiator reads the messages from a file, creates the envelope information and passes, without modification, the EDI message as the content of the mail. To create the X.400 envelope information, the initiation process uses information

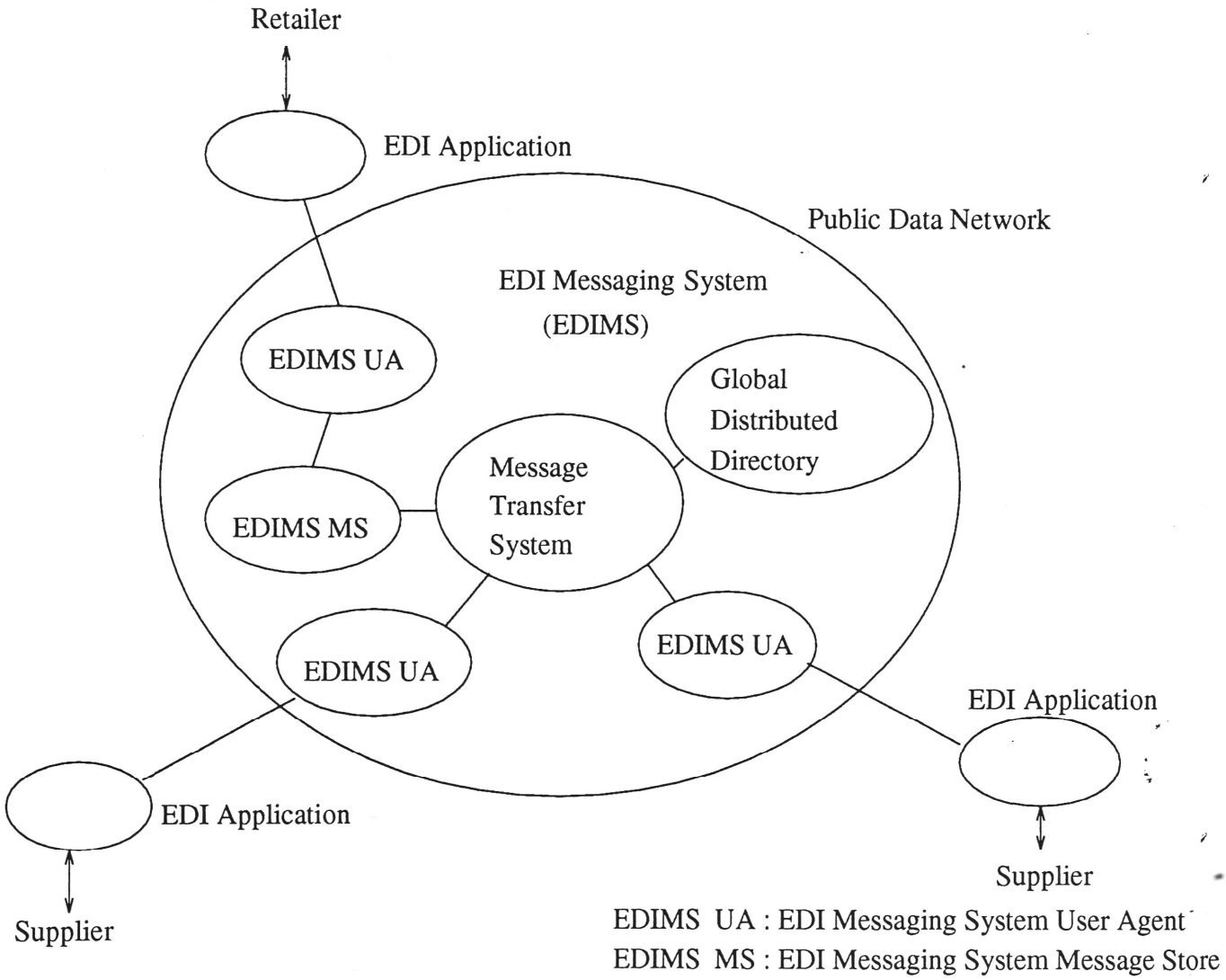


Figure 5.2: Functional Model of Direct Store Delivery System

from the contents of the X.500 Directory entries and the contents of EDI envelope messages. The envelope messages provide the distinguished name of the X.500 entries that contain the envelope information. The initiator process does not interpret any part of the actual EDI message. In theory, any EDI content could be sent. The initiator process can also process files containing multiple EDI messages but each message is sent in its own X.400 envelope. Once it has built the X.400 envelope, the initiator process passes the EDI message as X.400 mail to the service provider. More than one envelope message can be used depending upon the transaction.

5.1.2 Routing of Messages

The service provider routes X.400 mail for the EDI through the EDI Messaging Environment. In particular, the service provider uses the Originator/Recipient address (i.e. the trading partner's O/R address), the Message Transfer Agent and other entities in the X.500 Directory to find the route to the recipient. These routing entries must be configured for the EDI mail. The router also uses entries from its local routing information to find the route and other entities that define the receiving MTA to ensure that the routing path supports the X.400 mail. The trusted third party also provides a mail box for receiving the messages from the other trading partners.

5.1.3 Receipt of the EDI Message

The X.400 EDI messages must be received by the third party service provider and retrieved from the mail queue identified by a command to receive the mail. The receiver process uses an entry in the local MTA's routing information to determine if the address is local and to find a processing queue required by the

EDI message. It then opens the X.400 envelope, provides some basic verification of the X.400 messages and saves the content of the EDI message, without modification. Also the delivery response is sent to the originator conforming the receipt of the message. The auditing of the whole process is done by the third party service provider and the user is able to keep the a log of all the transactions.

The proposed model does not offer an interactive EDI solution as the messages are delivered on a store and forward basis. The third party service providers provide the users with mailboxes and the transactions can be dumped into the mailbox of a trading partner who can later retrieve it for processing.

5.2 Summary

The Direct Store Delivery System Model presents a cost effective solution for carrying out business using EDI on a global basis. In the next chapter the security involved in transmitting EDI messages over communications networks and a proposal to enhance the security in these systems is discussed.

Chapter 6

Security in EDIFACT

This chapter describes the UN/EDIFACT standards for structuring EDI messages. It discusses the security in the existing EDIFACT standard with the proposal to enhance the security in EDIFACT standards by incorporating certificates, digital signatures and security purposes in the messages itself.

6.1 Basic Concepts

In chapter 2, EDI has been defined as the application-to-application exchange of electronic data across organizational boundaries, in such a way that no human intervention or interpretation is required. The development of standards is a crucial factor in the EDI systems. The EDI standards provide the structure required for computers or, more specifically, applications running on computers to be able to read and process electronic data. For example, supermarket items come from different suppliers either directly or through wholesalers. The supermarket issues purchasing orders daily, which are sorted and distributed to its suppliers. The supermarket does all the trading through EDI for quicker delivery and overall accuracy in ordering. To carry out transactions smoothly

between various suppliers, they should have an agreed standard to format the data and exchange other forms of information like invoice, payment orders etc. Since there is no human intervention in EDI, it becomes necessary to develop an internationally standard in EDI to satisfy the needs of the large customers and the suppliers scattered globally. There are various standards developed to cope up with this problem of incompatibility, e.g. ANSI X12, UN/EDIFACT, ODETTE etc. The UN/EDIFACT standard has been accepted by the ISO as the universal standard for all document translation activities world-wide.

6.2 EDIFACT Standard

The UN/EDIFACT standard [36, 41]specifies syntax rules for EDI for administration, commerce, and transport to structure the EDI messages.

The document structures used in the standards have generally been unified, introducing principles and rules for their specification. Moreover, every document is suggested in the standard in terms of its structure and the properties of the structural components. In this way, these standards should cover all situations emerging in practice.

The EDIFACT syntax [41] defines the elements used to structure exchanges of data as shown in figure 6.1. It consists of one or more *Messages*, each related to a particular transaction, grouped together in an *Interchange*. The Interchange is an outermost envelope, and contains information about the sender and recipient (addressing) in the header, and about the total number of Messages in an Interchange in the trailer. This structure is just like having records in a data file.

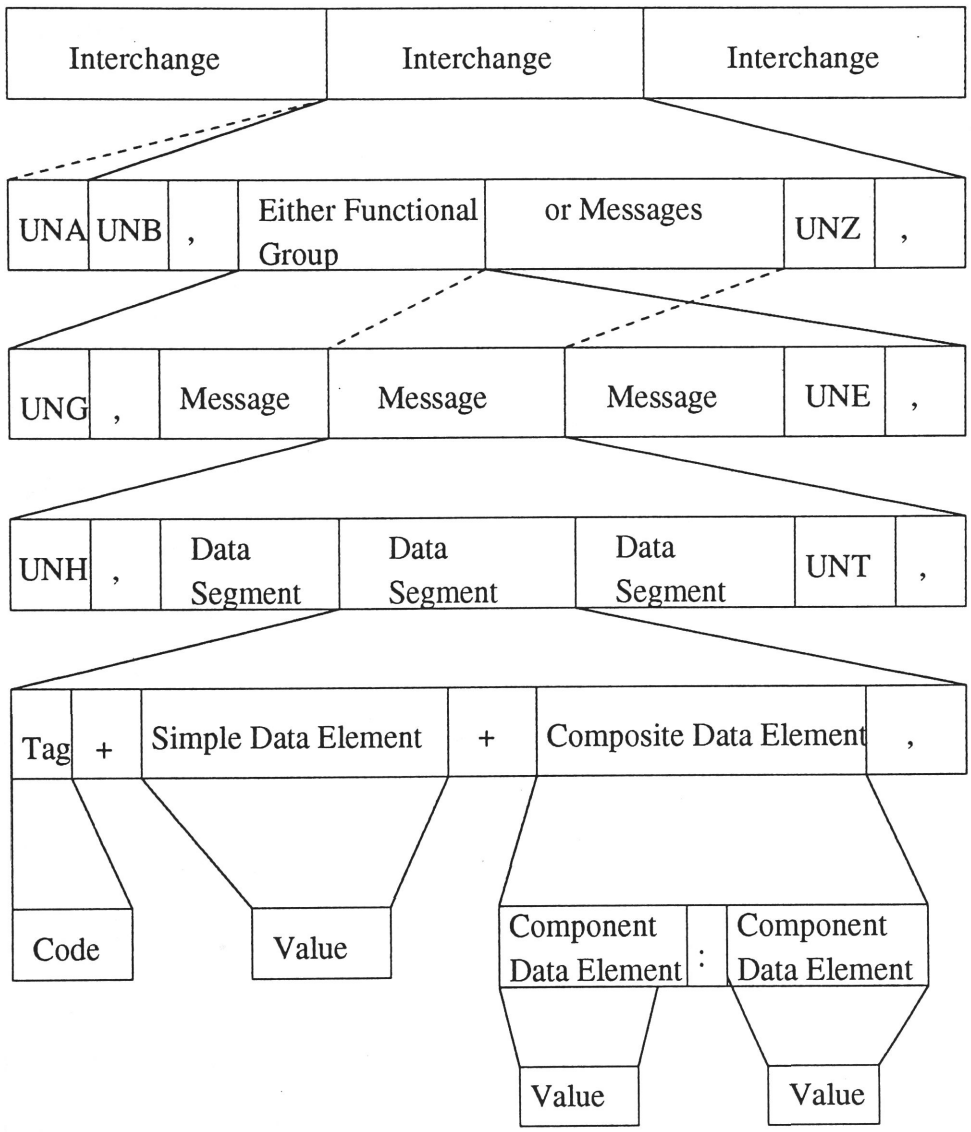


Figure 6.1: EDIFACT Structure

Messages themselves are formed from *Segments*, which in turn are built from *Data Elements*. The Data elements are identified by their position in the Segment, as indicated by the number of Data elements separators, and can be of variable length. Segments are identified by three characters (the tag) at the beginning and have their own Segment separators. They can also repeat. Their use may be either mandatory or conditional depending on the transaction taking place or the data to be conveyed, e.g. financial transactions, invoices, purchase order etc.

The message is the innermost envelope, and has a header which specifies the type of message (e.g. payment order, invoice) and a trailer which counts the number of segments in the message. The Interchange and the Message headers and trailers are also Segments. Since their three latter tag starts with the letter U, they are known as *Service Segments*, which are held in the *Syntax Directory*, rather than the *User Directory*, which contain *Message Segments*.

Thus, qualitative and quantitative information is contained in separate fields. Besides their value, they are assigned some meaning and properties, for example data format attributes. Different levels of nesting of the segment groups and segments are allowed to make parts of a document dependent on hierarchically higher segment levels.

6.3 Security in EDIFACT

The EDIFACT security documents [37, 38, 39] defines practical implementation of various EDIFACT security services within the message themselves. The

features offered by the standards include the following:

- independence of and transparent to the communication medium used;
- an open standard which supports all existing security mechanisms;
- the employment of security mechanisms such as confidentiality, authentication, integrity, non-repudiation etc. at application level;
- security services to be implemented by trading partners themselves, end to end and transparent to the underlying communication protocols, which may themselves provide security services;
- without making changes to individual messages. A global approach is adopted which can be applied to any message irrespective of the business application.

The basic security services used to protect an EDI message are:

Message Content Integrity

Message Content Integrity guarantees detection of unauthorized data modification of a message. It is achieved by sending with the message an integrity control value. This value is computed by using the asymmetric algorithms. The receiver of the message computes the integrity control value of the data actually received, using the corresponding algorithm and parameters and then compares the result with the value received.

Message Sequence Integrity

Message Sequence Integrity prevents duplication, addition, deletion, loss or replay of messages. It is guaranteed with a message sequence number or a

timestamp added to the message. In order to give full protection, the integrity of a sequence number or a timestamp must be guaranteed.

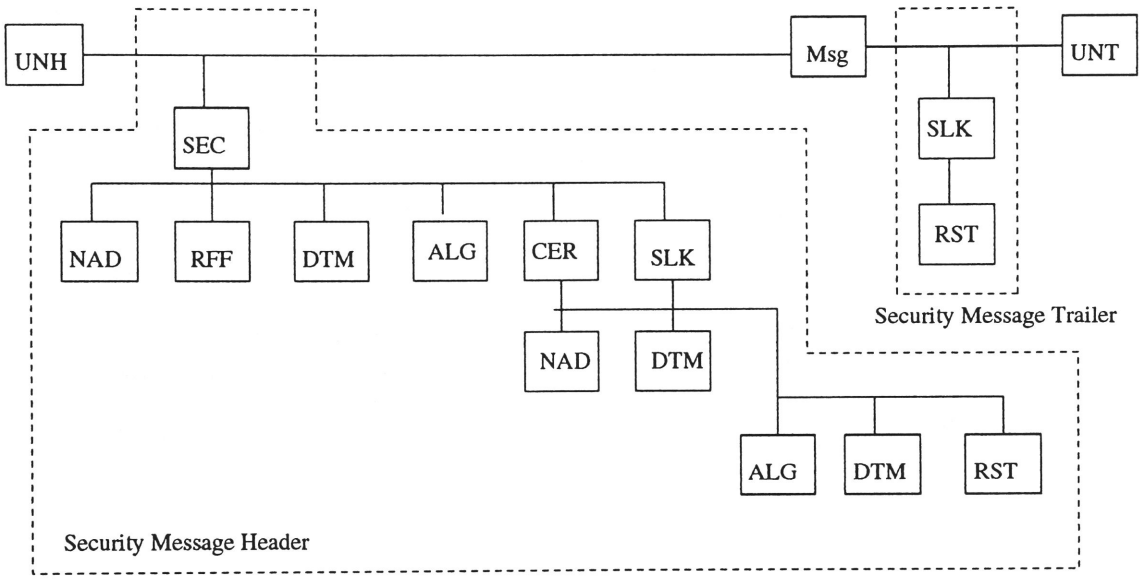
Message Origin Authentication

Message Origin Authentication protects against the actual sender of the message claiming to be some other authorized entity. It authenticates the origin of data and gives to the recipient the proof that the source of data received is as claimed. Message origin authentication is achieved by sending the digital signature along with the message.

6.3.1 Message Level Security

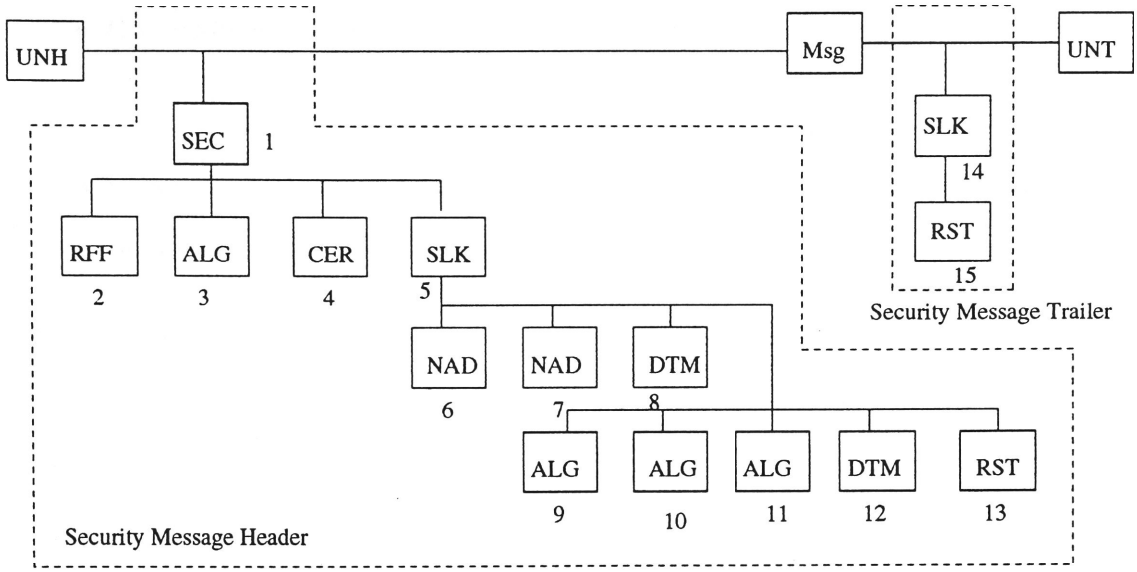
Security is incorporated in the individual messages. In EDIFACT standard, specific groups of security segments for message level protection are introduced. These security services are interpreted in the messages with the help of security headers and trailers. These segments can be used with any EDIFACT message. They are placed just after the message header and before the message trailer segments (UNH and UNT). The headers and trailers are actually a group of segments and can repeat, depending on the security needed, in any particular transaction. The overall structure of the security header and trailer is as shown in figure 6.2.

The security message header and trailer are reported for all the security services applied to protect the message. For example, a message may be secured by several entities and so the security related information may be repeated to allow the identification of several signing or authentication entities and correspondingly to include several digital signatures or control values. This approach allows maximum flexibility.



UNT : Message Trailer
UNH : Message Header
SEC : Security Mechanism
NAD : Name and Address
RFF : Reference
DTM : Date/Time/Period
ALG : Security Algorithm
CER : Certificate
SLK : Security Result List
RST : Security Result
Msg : Standard Message

Figure 6.2: Security in EDIFACT



SEC 1 : Authentication of Origin
RFF 2 : Security Sequence Number
ALG 3 : Hash Function to Sign + Parameters
CER 4 : Certificate of signer
SLK 5 : Number of Security Header
NAD 6 : Sender that generates digital signature
NAD 7 : Certification Authority
DTM 8 : Time of Validity

ALG 9 : Signature Algorithm of Message
ALG 10 : Hash function of Certificate Signer
ALG 11 : Signature Algorithm of Certificate
DTM 12 : Date of Issue
RST 13 : Certification Signature
SLK 14 : Number of Security Trailers
RST 15 : Digital Signature Value

Figure 6.3: EDIFACT Message Using the Digital Signature

The following procedure [46] outlines the use of public key cryptoalgorithm to ensure the origin authentication as shown in figure 6.4

- The sender server creates the digital signature of the message m to be transmitted.

  s=$hash(m)$

- The sending party signs the message digest (the digital signature) s using its private key K_s^c : $\tilde{s} = E_{K_s^c}(s)$

- The sender transmits (m, $\tilde{s}$)

- The resolver decrypts $\tilde{s}$ by using sender's public key $K_p^c = \ddot{s} = D_{K_p^c}(\tilde{s})$

- the resolver recomputes the message digest s = hash(m)

- if (s=$\ddot{s}$) then the resolver has validated the integrity and the originator of the message.

The run time for the public key cryptoalgorithm is quite high. Many CPU cycles are needed. Hence, we take the fixed size of the output of the algorithm i.e. the hashed contents of the message. A strong hash function should have the following properties:

- The hash function must be one-way i.e. given any possible hash result it must be computationally infeasible to construct an input message which hashes to this result (examples are the MD2, MD4, MD5 and HAVAL algorithms)

- the signature (message digest) produces a fixed length output.

- the hash function must be collision-free, i.e. it must be computationally infeasible to construct two distinct input messages which hash to the same result.

For example, a digital signature or MAC is introduced in the security message itself without changing the syntax of the EDI message. In the figure 6.3, the digital signature is added to provide authentication of origin. In detail, the security header contains:

1. The type of security function provided, e.g. authentication, integrity.

2. Whether security acknowledgment is required.

3. The character set used to represented the printed characters when the result was calculated, e.g. ASCII, EBCDIC.

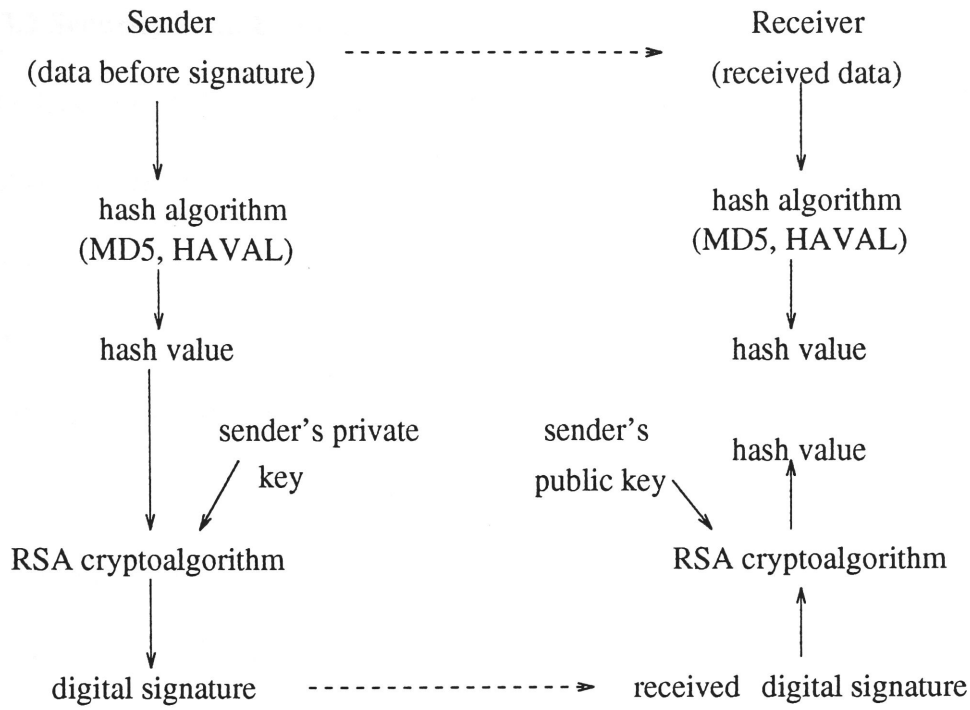


Figure 6.4: Digital Signature Generation and Validation

4. The roles of the security provider, e.g. issuing the message, witnessing their message.

5. Identification of security sender and recipient, e.g. who signed the message.

6. A sequence number and/or a timestamp.

7. The algorithms used to calculate the security result. e.g. RSA [1], MD5, DES.

8. A number to link the header to the corresponding trailer.

The security trailer contains:

1. The security result, e.g. MAC or digital signature.

2. A number to link the trailer to the corresponding header

6.3.2 Security Data Elements

The UN/EDIFACT security recommendations employ a considerable number of optional segments and data elements. In addition to that, some data elements have large field length definitions. This allows for the accommodation of all known security techniques and also possible evolutions thus providing the user with maximum flexibility in implementing the security mechanisms. However, once the user selects the appropriate security services to use, only a small subset of segments and data elements will be utilized and the actual size of the data elements would be shorter. The most important segments in the data elements are

SEC

Security service is actually provided, e.g. authentication of origin, message content integrity etc.

ALG

Identification techniques and algorithms used.

CER

Technical parameter required, e.g. certificates, key identification, user name etc.

RST

Security results e.g. MAC, integrity value, digital signature etc.

The approval of using the security segments for the message security level does not require syntax changes to the EDIFACT messages. The solution consists in the definition of the EDIFACT rule that states the acceptance of two approved forms of each existing EDIFACT message : one with security and one without

security. If the message must be secure then the security features must be in accordance to the recommendations of EDIFACT.

The two security services, not addressed by this structure, are the non-repudiation and the confidentiality of the messages.

Non-repudiation of messages require the recipient to issue and acknowledgment message which is signed by them. This special service is known as AUTACK (Authentication and Acknowledgment). It contains the same segment as in the EDIFACT standard to allow the recipient to sign the message, whilst the message itself contains unique references to the messages of the sender. This unique reference is usually composed of the message number (from the message header) and the security result (from the message trailer). Many original messages can be acknowledged by a single AUTACK. The AUTACK message has a second purpose. If the message is originally sent without security, it can subsequently carry a signature or a MAC for that message and the calculated hash value of the message. It is used sometimes where bulk data is sent, then the transactions are authorized and authenticated afterwards. It also provides a means of signing the whole interchange,until the security of the interchange level is used in the syntax.

Confidentiality is addressed by the introduction of a new message. The reason is that if all the data between the message header and the trailer is simply encrypted (and filtered to produce only the valid syntax as defined in EDIFACT), then the count on the number of the segments in the message trailer no longer matches the number of segment separators in the message. This may confuse some networks

and translators. For this reason, the whole of the original message, including all the headers and the trailers, is encrypted and filtered, and the result is put into a string of 350 byte free text segments. The security header is added, to describe the security originator and recipient, the encryption algorithm, filter function used and possibly the message encryption keys protected by public key techniques. When security is incorporated in the EDIFACT syntax, it is possible to introduce this header information to the normal message security header and also to the message to be encrypted.

6.4 Summary

In the Direct Store Delivery System, it is possible to incorporate EDIFACT message structures with enhanced security functions [38]. The secure EDIFACT message will include the following functions:

- Generation and storage of asymmetric cryptographic keys (in the form of X.509 certificates).
- Distribution of certificates from the administrator's station where certificates are generated to EDI servers(by ftp protocol)
- Generation and handling of symmetric cryptographic keys for encryption and integrity of EDI messages.
- encryption and integrity of outgoing messages, together with signing of the symmetric keys and
- verification of the signature of the symmetric key on receipt, decryption of the message and their integrity verification.

In the next chapter, the security in the communications networks is discussed. The issues of authentication, non-repudiation, integrity and confidentiality will be addressed.

Chapter 7

Security Services

This chapter describes the security services provided by the proposed model in an EDI environment. The model primarily provides security functions like mutual authentication based on X.500 standards, user identification, non - repudiation of origin and receipt for transferring EDI messages.

7.1 EDI Security Implementation

Security of a distributed system is a topic of growing importance. The security breaches of the last few years (internet worm) have demonstrated the need to have strong security policies and techniques to ensure reliable communication. The goal of any system is to carry transactions in an open and secure fashion either on a point-to-point basis or on a public data network. The crucial question that needs to be addressed before implementing the security services, is their placement at appropriate level in the ISO/OSI reference model. Given the nature of the type of security processing to be performed (e.g. integrity checking), it is essential that the security mechanisms be invoked while the entire EDI information segments is still intact. The reasons for locating the

security services in the model at the application level are:

- they satisfy security requirements which are inherently meaningful only to a particular application, e.g. access control to application-internal resources, or non-repudiation;
- protect selected fields within application protocols, e.g. the PIN in a financial transaction;
- protect information conveyed through multiple end systems in distributed applications, e.g. application level store-and-forward; and
- provide end-system level protection, without forcing an application to depend on a particular underlying protocol (e.g. the OSI transport or network protocol).

7.2 Assumptions

The security services are based on the X.400 and X.500 standards. In providing the security services in the model of the *Direct Store Delivery System*, it is assumed that the Directory is free from tampering and the certificates obtained from the Directory are unforgeable. The following assumptions are made in the X.500 standards for the secure exchange of certificates:

- A secure bind from the Directory User Agent (DUA) to a Directory Service Agent (DSA); this is a secured Directory Access Protocol (DAP).
- If two DSAs are to communicate with each other, they may do so by a secured access between them of the Directory Systems Protocol (DSP).
- If the DUA requests information which is not on the DSA to which it is bound, that DSA may request the information from other DSAs

by secured DSP enquiries; the data will not be returned to the DUA (referral); the DUA may then make a strong bind to the referred DSA with DSP.

7.3 Computer Security Planning for EDI

The network service provider should provide the protocol conversion and mail box facility for storing messages of the various trading partners. In addition, the basic security services and audit trails should be kept by the trusted third party [32].

7.3.1 Risk Based Implementation

In the development of computer security plans for EDI, agencies should allocate resources according to the risk and magnitude of potential harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained or transmitted by the EDI system. In EDI, certain types of messages may be more inherently sensitive than others. There must be assurance that each price quotation or purchase order is accurate and has been sent from the named originator. Less care would need to be taken with invoice sent to an agency, if the agency's internal control system is sufficiently robust to automatically reject all non-authentic invoices.

7.3.2 Maintenance of Electronic Records

EDI messages that are transmitted must be included in the system of electronic records. It must be ensured that :- the records of EDI interchanges are complete; unauthorized modification or alterations to records are prevented;

all modifications or alterations are automatically recorded in an electronic audit trail and dates and times of relevant activities are recorded and are correct and precise.

7.3.3 Audit Trail for Message Authorization

With the paper documents that are sent to the recipient, the handwritten signature of an authorizing officer is usually used to obligate the originator; a notation that the original was signed is often seen on a retained copy. An equivalent must be provided for each EDI message used as a replacement. An electronic copy of each transmitted EDI message, together with the proof of approval, should be retained for audit purposes.

7.4 Security Services

7.4.1 User Identification

To use the EDI system services, the user has first to identify his credentials to the server. Once the credentials are established, the user can use the services to either query the database or carry out other transactions. There are two practical approaches in the user identification.

In the first approach, the user, after entering the name, is prompted for a password which consists of the user's name, a one-way hash of the password, a timestamp and a nonce which is returned to the user to be used . To prevent the hash of the password and the nonce from being intercepted over the network, they are encrypted using the public key of the CA. If the one way hash of the password from the database matches with that of the user, the CA

returns the nonce encrypted with the public key of the originator.

The second approach is used in retail stores which use a standalone PC for communicating EDI messages. To identify the individuals responsible for signing the transactions, a personal token such as smart cards [47] can be used for user identification. Smart cards are unforgeable and provide reliable means of identification.

7.4.2 Authentication

Authentication is used to:

- verify the identity of the sender of a message to the receiver in order to detect spoofing or impersonation.
- verify the integrity of the message by detecting changes (modifications) in a message introduced between the sending and receiving process.
- protect a unique message identifier used to detect attempts at insertion, deletion or replay of messages.

Most of the above threats can be countered by using strong authentication. In this, neither the entity which is authenticated nor any eavesdropper on the conversation can furnish the ability to impersonate the authenticating principal. There are some interception attacks which cannot be countered by strong authentication only. Hence, additional data encryption is needed to secure the channel. The well known cryptosystems are RSA using public key techniques and DES, LOKI using symmetric key techniques. RSA is a widely preferred algorithm for digital signatures as well as for authentication with secrecy.

The message-origin authentication service is provided by the existence of the message token containing the signature which uniquely identifies the origin of the message. To achieve this, *the content integrity check* is included in the signed data part of the token.

The receiver obtains the trusted copy of the public key from the Certification Authority of the sender. If the CAs of the sender and receiver are different then the receiver uses the certification path that has been supplied as a part of the originator's certificate, to determine the copy of the receiver CA's public key. Using this the receiver validates the signature on the originator's certificate.

7.4.3 Authentication Protocol

The X.509 Directory Authentication framework is defined in the standards. This protocol is a slight modification of the standard mutual protocol [15] due to the security defects mentioned in the existing X.509 protocol [27, 30, 45].

Notations:

CA	Certification Authority
E	Encryption
D	Digital Signature
R_C	Nonce by C
k_c^s	Secret Key of C
k_c^p	Public Key of C
t_1	timestamp

h(X)	hashed content of message X
$data_c^1$	plaintext data from C
$data_c^2$	encrypted data from C
D_1	$D(k_{CA}^s, A.k_a^p.t_1.t_2)$
D_2	$D(k_{CA}^s, B.k_b^p.t_1'.t_2')$
.	Concatenation

The exchange between the two parties A and B starts with A sending a message to the Certification Authority (in this application the Third Party who acts as a CA) to find the public component of B [2].

$$
\begin{array}{lll}
Step1. & A \rightarrow CA & A.B \\
Step2. & CA \rightarrow A & D_1.D_2 \\
Step3. & A \rightarrow B & D_1.R_A.B.data_a^1.E(k_b^p, data_a^2).D(k_a^s, \\
 & & h(R_A.B.data_a^1.E(k_b^p, data_a^2)) \\
Step4. & B \rightarrow A & R_B.A.R_A.data_b^1.E(k_a^p, data_b^2). \\
 & & D(k_b^s.h(R_B.A.R_A.data_b^1.E(k_a^p, data_b^2))) \\
Step5. & A \rightarrow B & R_B.D(k_a^s.h(R_B, B))
\end{array}
$$

In the second step, the CA sends A, the certificates of both A and B. In order to sign data, the user applies a one-way hash function to the data followed by the digital signature D. Timestamps are needed to guard against the replay attack [3]. An intruder is not able to replace the messages in the above steps since he does not have the secret key of the CA. In the third step, A generates a nonce R_A, which is used to detect replay attacks and to prevent forgery. Additionally A can send some plaintext data $data_a^1$ which he signs to preserve the integrity and some secret data $data_a^2$. On receiving the message from A, B verifies the certificate, checks that B itself is the intended recipient, timestamp is current and optionally checks whether R_A has not been replayed.

B then generates a nonce R_B for similar purposes to R_A. Additionally B can also send some plaintext data $data_b^1$ and secret data $data_b^2$. A checks that A is the intended recipient, R_A is identical to the one which was sent by A and the R_B is not been replayed. It responds to B by sending the nonce R_B along with the B. On reception, B checks the signature and thus the integrity of the signed information and also checks that R_B is identical to the one which was sent by B.

In this way, at the end of the protocol, both the users are convinced that they are communicating with the right person. The above authentication process safeguards the integrity as well as confidentiality of the message. The users can then generate a session key which is used to encrypt the subsequent traffic on the association.

7.4.4 Non-Repudiation

Non-repudiation of origin protects the recipient from the sender's denial of having ever sent the message. Protection can be achieved by the sender including the digital signature with the message and the receiver sending the acknowledgment which contains the digital signature.

The non-repudiation of delivery does not necessarily imply that the recipient read the data or acted upon it in any way. The recipient can acknowledge the receipt by generating an acknowledgment message back to the originator, with the message containing the digital signature computed on a copy or a digest of the contents of the original delivered data item. Figure 7.1 shows the operation where the recipient's digital signature is used. The sender of the message requests this service from the receiver by by including a proof of delivery request flag as a part of the signed data in the message token to the receiver. The proof of delivery is computed as a signature on the unencrypted

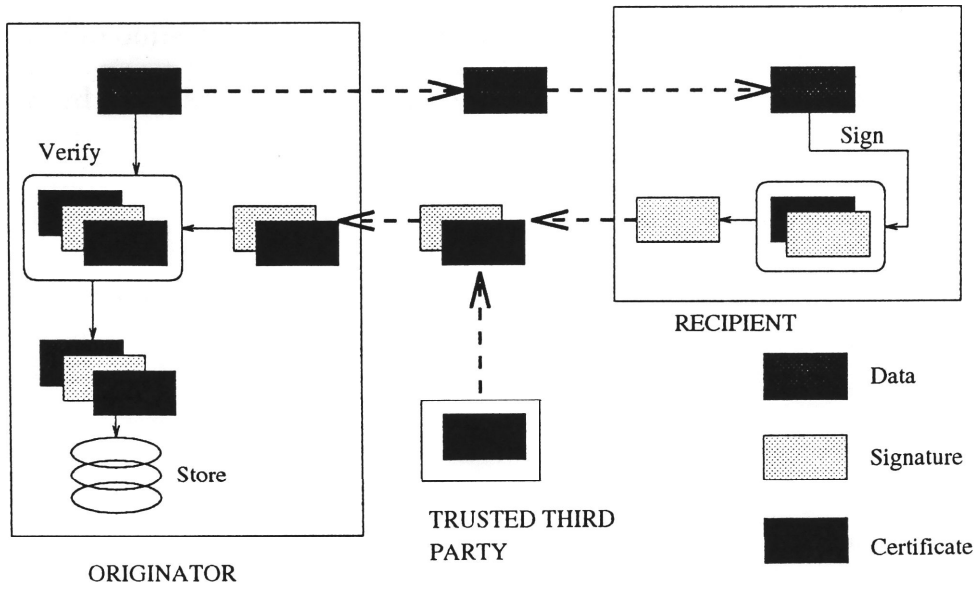


Figure 7.1: Non-Repudiation of Delivery

message content and the various other parameters. The receiver then returns the proof of delivery together with his certificate to the sender of the message.

7.4.5 Responsibility

A new feature in EDI MS is the EDI responsibility notification. The purpose of introducing the concept of EDIMS Responsibility is primarily to provide a method for confirming the passing of messages amongst UAs. In EDIMS a user or user application can request a notification of responsibility of a message by a recipient or a recipient application. This notification is requested by an originating UA and is generated by a recipient UA taking the responsibility for the message. Responsibility implies that a message received is either available to the EDIMS user or that it is forwarded with changes. One notification serves to carry both the positive response above and a negative response. The negative response means that the message referred to will not be processed by an EDI application. It is possible to forward a received message unchanged

and pass the obligation to respond to the responsibility notification request to the forward recipient, or intermediate recipients who then must respond to the originator of the message.

The Responsibility field is represented as :

ResponsibilityForwarded ::= BOOLEAN (Default FALSE)

If this field is TRUE it indicates to the receiving UA that Responsibility was forwarded. If this value is FALSE (or absent), it indicates to the receiving UA that the security elements of the inner envelope have been checked.

7.4.6 Key Management

Regardless of the type of cryptosystem used, either symmetric or asymmetric, it is necessary for the communicating parties to obtain each others keys. In the proposed model, the X.500 Directory services were used for the distribution of certificates which contain the public key of the trading partners. The advantage of using the Directory services is that the keys can be freely distributed in a networked environment.

7.4.7 Message Loss

Vulnerability to message loss is considered critical to an EDI application. The types of message loss can be distinguished as:

- failure of the UA or MS
- loss of individual message due to security violations

As a result, the transfer of messages between responsibility domains requires protection for service providers in addition to that of end users.

7.5 Summary

This chapter described the security services which are incorporated in the proposed model. The service, like authentication on a global basis, is realised with the use of X.500 standards. Also, the non-repudiation services, which are very important due to lack of a hard copy, can be effectively implemented by the use of digital signatures.

Chapter 8

Conclusions and Further Work

In this thesis, a model of the *Direct Store Delivery System* was proposed which can be implemented in a cost effective manner without compromising the security of the Electronic Data Interchange Systems. The security provided in the existing EDI systems were studied and a proposal was made to enhance the security in the present day EDI system which incorporated the enhanced security services like mutual authentication, non-repudiation, responsibility, user identification etc.

The whole EDI transaction was divided into two distinct categories:

- The conversion of the in-house application into an EDI format with the use of translation software. The security features provided in the UN/EDIFACT standard for structuring EDI messages are enhanced with the inclusion of the certificates and digital signature, without changing the syntax of the EDI format. Single or multiple messages level security can be incorporated in the model. Thus the security provided will depend on whether a financial transaction or any general EDI transaction is taking place.

- After the conversion into a standardized EDI format, the EDI messages needs to be communicated over a communications network. The inherent security problems in the network makes it necessary to have security while the data is in transit. Also in a distributed networked environment, reliable authentication between the communicating parties is necessary. In this model global authentication was provided by the use of X.509 Directory Authentication framework and the whole transaction can be carried out in a message handling system.

The third party service providers are responsible for the basic services of keeping the log of transactions, audit and other control functions. Also, they can act as a Certification Authority to keep the database of user information which can be freely communicated on a network.

As a result of the security enhancements, the problems occurring in the the EDI systems like cross vulnerability, password guessing attacks, authentications can be countered efficiently. In general, the following features are provided:

- The *Direct Store Delivery System* is a straight forward model which provides a high degree of security in a cost effective manner.
- It relieves the user from the burden of maintenance, upgradation of the system and expansion to other networks.
- If the third party service providers have the provision of Directory services and messaging handling systems, then the electronic transactions can be carried out globally with a reasonable degree of security.
- Once the user authentication is complete, all the security features of the model will be transparent to the user.

- In the model, we make no assumptions about the security of the underlying network. The data is transmitted in an encrypted form to ensure that even the third party cannot extract message enroute.

8.1 Further Work

The next step is to implement the *Direct Store Delivery System* by providing a Graphical User Interface (GUI) tool. In the current application, the model cannot be used in an interactive mode but this is not a major limitation. Secondly, the RSA public key cryptosystem is used for exchange of certificates and public keys. The RSA cryptosystem is slower than the conventional cryptosystems, but as the application is not interactive, the computational time delay is not noticed by the user.

The security features should protect all types of data. Future EDIs must be able to deal not only with standard business data but also with related data such as electrical and mechanical characteristics (CAD/CAM and test data).

Bibliography

[1] R. Rivest, A. Shamir and Adleman. A Method for obtaining digital signatures and public key crypto-systems, *Communications of the ACM*, Vol. 21, no. 2, pp 102-126, 1978.

[2] R. Needham and M. Schroeder. Using Encryption for authentication in large network of computers, *Communications of the ACM*, Vol. 21, no.12, pp 993-999, 1978.

[3] D. Denning and G. Sacco. Timestamps in Key Distributed Protocols, *Communication of the ACM*, vol 24, no 8, pp 533-535, 1981.

[4] J. Tardo and K. Alagappan. SPX: Global Authentication Using Public Key Certificates, *IEEE Symposium on Research in Security and Privacy*, pp 232-244, 1991.

[5] B. Jerman-Blazic. Security in Value Added Networks, Security Requirements for EDI, *SBT/IEE International Telecommunication Symposium*, pp 361-365, 1990.

[6] M. Toussiant. Analyzing Security of Cryptographic Protocols, *IEEE Journal on Selected Areas in Communications*, Vol. 11, No. 5, pp 702-714, 1993.

[7] G. Dickson and A. Lloyd. *OSI*, Prentice Hall of Australia Pty Limited, ISBN 0-13-640111-2, pp 279-283,303-307, 1992.

[8] C. Mitchell and A. Thomas. Standardizing Authentication Protocols Based on Public-Key Techniques, *Journal of Computer Security*, pp 23-36, 1993

[9] C. Mitchell, D. Rush and M. Walker. A Secure Messaging Architecture Implementing the X.400, 1988 Security Features, *The Computer Journal*, Vol 33, No. 4, pp 290-295, 1990.

[10] P. O'Grady. *Putting the Just-In-Time Philosophy into Practice*, Kogan Page Limited, London, ISBN 1 85091 121 5, 1988.

[11] S. Kent. Internet Privacy Enhanced mail, *Communication of the ACM*, vol 36, No. 8, pp 48-60, 1993.

[12] D. Gaon, K. Eller, W. Free and F. Ogden. Concept of Implementing A Globally Distributed X.500-Based DoD Directory, *MILCOM'92 Communication -Fusing Comand, Control and Intelligence Conference Record*, pp 1195-1199, 1992.

[13] A. Marcella and S. Chan. *EDI Security, Control and Audit*, Artech House, 1993.

[14] D. O'Mahony. Security Considerations in a Network Management Environment,*IEEE Network*, pp 12-17, 1994

[15] Information Processing Systems - Open Systems Interconnection - *The Directory Authentication Framework.* ISO/IEC 9594-8:1993, also CCITT 1988 Recommendation X.509.

[16] CCITT Recommendations Message Handling Systems : *Electronic Data Interchange Messaging System Recommendations X.435*, 1991.

[17] V. Varadharajan. Security in a Distributed Message Handling System , *IEE Colloquium on 'Message Handling - Past, Present and Future'*, pp 5/1-9, 1991.

[18] *C.C.I.T.T. Draft Recommendations X.400, Message Handling Systems - System and Services Overview*, Version 5.5, April 1988.

[19] M. Purser. *Secure Data Networking*, Artech House Inc. , MA, 1993.

[20] W. Ford. *Computer Communications Security : Principles, Standard Protocols and Techniques*, Prentice Hall Ltd, NJ ,1994.

[21] S. Muftic(et al.) *Security Architectures for Open Distributed Systems*, John Wiley and Sons., UK, 1993.

[22] *Electronic Data Interchange : Streamlining Business Communications*, Computer Technology Research Corporation, USA, 1993.

[23] P. Swatman. Integrating Electronic Data Interchange into Existing Organisational Structure and Internal Application Systems: the Australian Experience, Phd thesis , 1993.

[24] G. Simmons. *Contemporary Cryptology : The Science of Information Integrity*, IEEE Press New York, 1992.

[25] J. Barkley. Security in Open Systems, *NIST Special Publication 800-7*, Computer Systems Technology, US Department of Commerce, NIST, October 1994.

[26] C. Mitchell, D. Rush and M. Walker *CCITT/ISO Standards for Secure Message Handling*, IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, pp 517-524, 1989.

[27] C. Mitchell and C. I'Anson. Security Defects in CCITT Recommendations X.509 - The Directory Authentication Framework, *Computer Communication Review*, vol 20, no. 2, April 1990, pp 30-34.

[28] C. Pfleeger. *Security in Computing*, Prentice Hall International Inc.,NJ, 1989.

[29] J. Steiner, C. Neuman and J. Schiller. Kerberos : An Authentication Service for Open Network Systems, *Proceedings of USENIX Winter Conference*, pp 191-202, February 1988.

[30] M. Burrows, M. Abadi and R. Needham. A Logic of Authentication, *Research Report 39*, Digital Systems Research Center, Palo Alto, California, A condensed version of this report appeared in *ACM Transactions on Computer Systems*, Volume 8, No. 1, pp 18-36, February 1990., February 1990.

[31] J. Cobb *Security Implications in Electronic Data Interchange* IEE Colloquium on 'Standards and Practices in Electronic Data Interchange' (Digest No. 106), pp 7/1-4, 1991.

[32] Security Issues in the use of Electronic Data Interchanges, *CSL Bulletin* from the site http://www.csl.nist.gov, June 1991.

[33] B. Schneier. *Applied Cryptography : Protocols, Algorithms and Source Code in C*, John Wiley and Sons, New York, 1994.

[34] S. Bellovin and M. Merritt. Limitations of the Kerberos Authentication System, *Proceedings of USENIX Winter Conference*, pp 1-16, 1991.

[35] V. Voydock and S. Kent. Security Mechanisms in High-Level Network Protocols, *ACM Computer Surveys*, 15(2), pp 135-171, June 1983.

[36] J. Berge. *EDIFACT Standards*, NCC Blackwell Limited, 1991.

[37] B. Di Turi. Security in EDIFACT Messages, *Computers and Security*, vol 12, No. 5, pp 447-455, August 1993.

[38] T. Dosdale. Security in EDIFACT Systems, *Computer Communications Magazine*, vol 17, No. 7, pp 532-537, July 1994.

[39] Recommendations for UN/EDIFACT Message Level Security, UN/EDIFACT WP.4 Document, R.1026 Add 1, 1994.

[40] D. Zazula. EDI-PRO : An Integrated Environment for Electronic Data Interchange, *Computer Communications Magazine*, vol 17, No. 12, pp 876-885, December 1994.

[41] EDIFACT - Application Level Syntax Rules, ISO-9735, ISO, Geneva, Switzerland, 1988.

[42] W. Caelli, D. Longley and M. Shain *Information Security Handbook*, MacMillan Publishers Ltd., UK, 1991.

[43] D. Gerberick. Working Paper on Functional Specifications for an EDI Cryptoserver, *Security Audit and Control Review*, pp 11-19, Summer 1991.

[44] W. Pugsley. Electronic Data Interchange - An Overview, *Proceedings of the International HP Users Conference*, Brussels, paper BU/OA/09, 1989.

[45] D. Coppersmith. Analysis of ISO/CCITT Document X.509 Annex D, IBM Research Division, Yorktown Heights, June 1989.

[46] C. Schuba and E. Spafford. Addressing Weaknesses in the Domain Name System Protocol, MS Thesis, Purdue University, USA, August 1993.

[47] J. Zoreda. *Smart Cards*, Artech House, Boston, USA, 1994.

[48] P.G.W. Keen. *Competing in Time : Using Telecommunication for Competitive Advantage,* Ballinger: Cambridge (Massachussets), 1986.

[49] J.C. Emery. *Management Information Systems : The Strategic Resource,* Oxford University Press, Oxford, 1987.

Appendix A

Security Enhanced Direct Store Delivery System

Abstract

Currently there is limited security provided in carrying out business using Electronic Data Interchange (EDI). The aim of this paper is to enhance the security of the Direct Store Delivery System which is a special form of EDI. The whole communication process is carried out using a trusted third party service provider with a view to maximize the performance of the system. The model describes authenticity using X.500 recommendations, confidentiality and integrity using public key cryptography and provides a low cost solution to the existing system. The transactions are carried out in the UN/EDIFACT format using the X.435 standards.

A.1 Introduction

The primary purpose of EDI is to provide communication standards that promote the interchange of common business information to facilitate the elec-

tronic linkages without human intervention. In recent years, both public and private sectors use EDI for trading purposes. The increasing use of EDI in financial transactions has made it necessary to consider network security in greater detail and enhance the security in these systems. The following issues need to be raised in view of security of the existing EDI systems [13].

- There is limited security in most of the present day EDI systems. They rely on passwords to access the system thus making it vulnerable to password guessing attacks.

- As more and more business information is transmitted between computer systems, we need to protect these transactions from unauthorized viewing and/or alteration. Unauthorized viewing can provide competitive information which may be undesirable to disclose. With the introduction of third parties and increased risk of unauthorized access to confidential information, there is a need to restructure the existing security features.

- Generally, EDI systems work on a point to point basis or have a limited number of trading partners. The security and control features incorporated in the system are as strong as the weakest link in the EDI chain. A cross-vulnerability resulting from technical limitation can compromise the integrity of the dependent EDI systems.

- Different security standards may create problems when trading partners are adhering to different standards.

- The security features needs to be upgraded as the complexity grows.

This paper describes security enhancement of the **Direct Store Delivery System** which uses a Trusted Third Party Service Provider or Value Added Network (VAN) over a network as shown in figure 1 with a view to maximize

the performance of the system. It provides a low cost security solution to the existing EDI applications. We used X.500 standards based on the Directory Services for resolving the address issues and mutual authentication based on the principal global identity [15]. The whole transaction in the model was carried out using the UN/EDIFACT format of transactions.

Section 2 provides the background on the concepts used in the model, section 3 describes the Direct Store Delivery System model and the security features provided and section 4 summarizes the paper with the gains in implementing the model and scope for further work.

A.2 Concepts and Mechanisms

The primary goal of any system is to carry out transactions in an open and secure fashion either on a point to point basis or on a public data network. However, in networked and distributed environments, what particular users are allowed to do depends upon the security policies in effect. Within a single domain, where all processing nodes and network links are under the control of the same administration, security is not such a critical issue. However, when the transaction takes place between two separate domains and makes use of public data networks, security issues must be considered in great detail. A trusted third party network provider provides some security functions like trusted key issuers, key-management facilities, user registration, notary services and security gateways.

A.2.1 Security Issues

The following are some of the network security issues which need to be considered for secure communication.

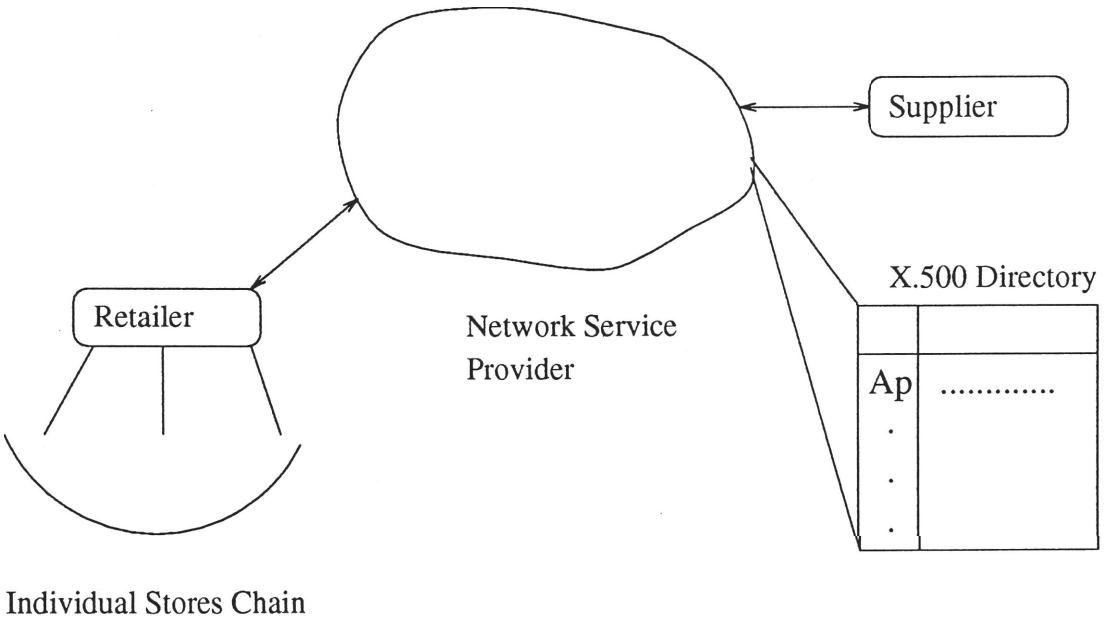


Figure A.1: Direct Store Delivery System

- Authentication

  Authentication is a process used to:

  - verify the identity of the sender of a message to the receiver in order to detect spoofing or impersonation.
  - verify the integrity of the message by detecting changes (modifications) in a message introduced between the sending and receiving process.
  - protect a unique message identifier used to detect attempts at insertion, deletion or replay of messages.

  Most of the above threats can be countered by using strong authentication. In this, neither the entity which is authenticated nor any eavesdropper on the conversation can furnish the ability to impersonate the authenticating principal. There are some interception attacks which cannot be countered by strong authentication only. Hence, additional data

encryption is needed to secure the channel. The well known cryptosystems are RSA [1] using public key techniques and DES, LOKI using symmetric key techniques. RSA is widely preferred algorithm for digital signatures as well as for authentication with secrecy.

- Key Distribution and Management

  Secure methods of key management are extremely important. In practice, most attacks on the public key systems are probably aimed at the key management levels, rather than at the cryptographic algorithm itself. Users must obtain a key pair securely and efficiently suited to their security needs. In compliance with the CCITT X.500 standards the directories contain certificates as well as the public keys. Certificates are unforgeable. Hence it is difficult to impersonate another user.

- Non-Repudiation of Origin and Receipt

  Non-repudiation of origin protects the recipient from the sender's denial of having ever sent the message, while non-repudiation of receipt protects the sender of the message from the receiver's denial of having received the message. Protection can be achieved by the sender including the digital signature with the message and the receiver sending the acknowledgment which contains the digital signature. In the protocol, the identity of the user is bound with the public key by digital signature by issuing certificates. The proof of delivery is done by the appropriate User Agent when it receives the message.

- Security Elements in EDI Messaging Structure

  The word envelope is used to represent different headers and trailers structured to form the EDI message as shown in figure 2. The UN/EDIFACT

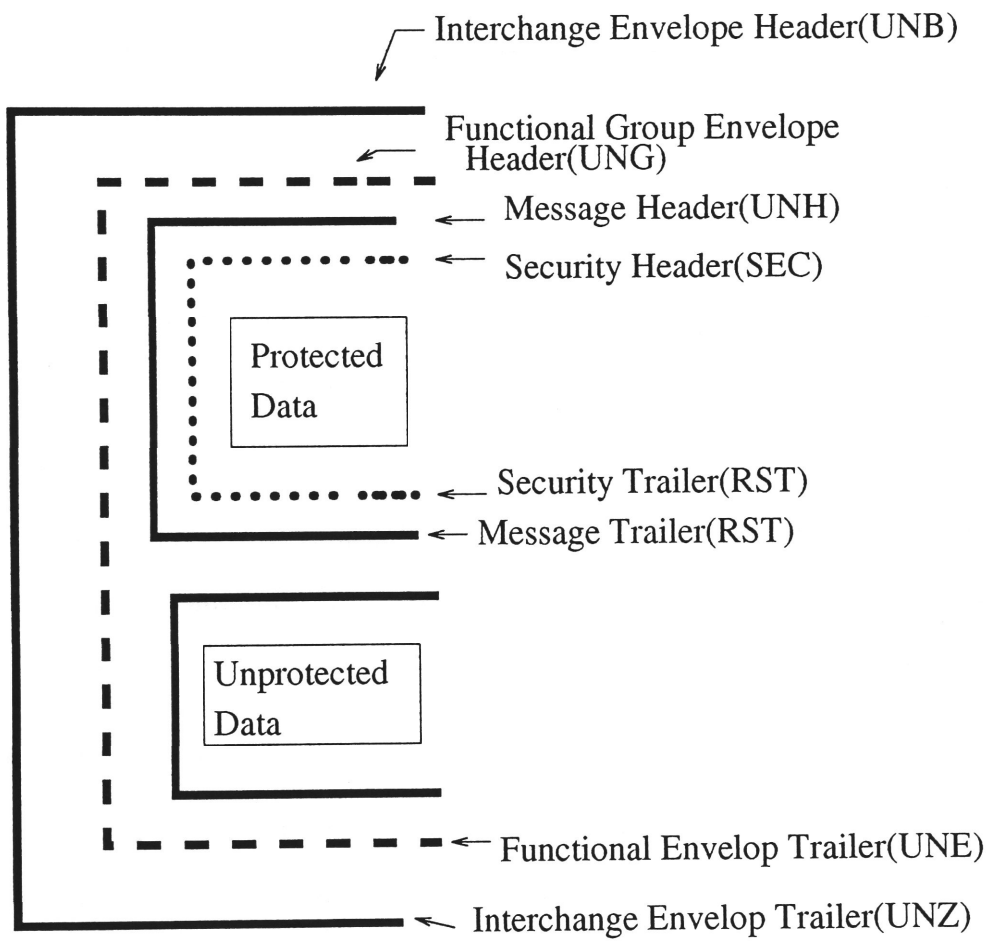


Figure A.2: UN/EDIFACT message format

standard provides the following features:

- the employment of established security mechanisms
- security services to be implemented by trading partners themselves, end to end and transparent to the underlying communication protocols, which may themselves provide security services
- independence of and transparent to the communication medium used
- an open standard which supports all existing security mechanisms
- not involving changes to individual messages. A global approach is adopted which can be applied to any message irrespective of the business application.

All security functions except the non-repudiation of receipt are provided by the inclusion of generic security header and trailer segments after the message header (UNH) and before the message trailer(UNT). If required a financial transactions can use more than one security envelopes.

- Responsibility

  Another important feature that is incorporated is the responsibility for messages at each stage of the message path through the Message Handling System environment [16]. Since a Trusted Third Party is used, the transfer of responsibility is to be clearly identified and assured of further protection not only to the end users but also to the service provider. In the X.435 standard, the Responsibility Forwarded field is used to indicate whether Responsibility was forwarded or not. When responsibility is accepted, the security elements are checked.

- User Authorization and Access Control

Authorization is an identity based access control for authorizing a particular user to carry out transactions. A simple way of doing this is to send the distinguished name and the password. The Directory will confirm whether the credentials are valid or not. The user is then notified accordingly. The proper functioning of the logical access control assists in preventing and detecting (by reporting security violations and attempts to access) unauthorized access to data.

A.2.2 The Directory

The Directory Services are required to support the security services within the message handling system and provide a name server. Typically, the MHS may access the Directory to determine the credentials of a user for the authentication process, identify the intended receiver and to resolve the address issues. The two basic entities of the Directory Service are the Directory User Agent and the Directory Service Agent.

Each user's public key is stored in the Directory. A user wishing to have a secure exchange of messages with another user, obtains the other user's public key by using the Directory Services. He then uses this key within the required security service. The directory should be secured against tampering. Users are allowed to view and query the database and only the Certification Authority is allowed to modify an entry in the directory.

The security services can be provided by different layers and different protocols depending on the application requirements. The approach is based on the following functions:

- identification of the vulnerabilities of the system
- definition of security services

- placement of the security services in the particular protocol.

A.3 The System Model

The Direct Store Delivery System [10] is a chain of stores where ordering and deliveries are carried out centrally and the chain handles the distribution to the individual stores. It uses EDI to place bulk order with the suppliers telling them how much to deliver and when. Thus the retailers continue to get the benefit of centralized ordering and like the use of Just-In-Time stock management techniques, reduces inventory and saves on warehouse and material handling costs. The merchandise can be ordered faster and a given item is never out of stock. At the same time there is increased vulnerability to illegal access with the use of public data network and a trusted third party.

The system consists of User Agent and Message Store in the messaging environment modeled as a functional object as shown in figure 3. The whole transaction process can be divided into independent processes:

- Service Initiation → Initiation process starts with the retailer logging into the network through the access units User Agents.

- Verification of Public key of the trading partner → The user can verify the public key of the trading partner from the database query and get the appropriate certificate from the directory database.

- Generation of the Session key for transactions → Once the authentication of the trading partners has taken place then they can generate a session key to encrypt the subsequent traffic on the association.

- Trading : After completing all the above processes, the user can carry out transactions. The transaction generated is dumped into the mail

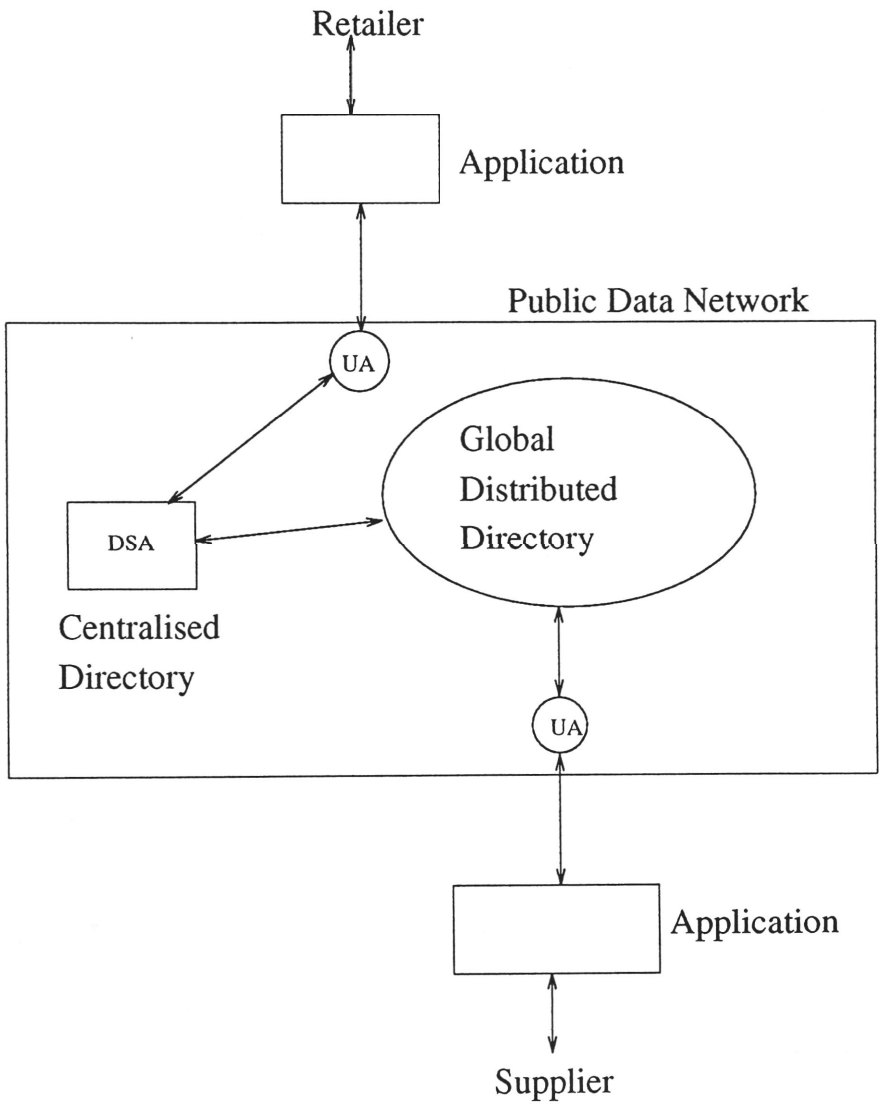


Figure A.3: Functional Model of Direct Store Delivery System

box of the supplier who processes it and sends an appropriate response to the request. The auditing of the whole process is done by the third party and the user keeps a copy of the log of the transactions.

The security requirements are related to the user's perceived threats and his assessment of the cost of the security breach. Keeping this in view, the following generic security services are added to the Direct Store Delivery System.

A.3.1 Basic Security Services

The message consists of two parts, namely an Envelope and a Content. The Envelope contains the necessary information for routing and delivering purposes and the Content contains the actual information which is to be transferred.

User Authorization

For using the services the user has first to identify his credentials to the server. Once the credentials are established, the user can use the services to either query the database or carry out other transactions. The user, after entering the name, is prompted for a password which consists of the user's name, a one-way hash of the password, a timestamp and a nonce which is returned to the user to be used. To prevent the hash of the password and the nonce from being intercepted over the network, they are encrypted using the public key of the CA. If the one way hash of the password from the database matches with that of the user, the CA returns the nonce encrypted with the public key of the originator.

Key Management

The RSA public key system is used to exchange the DES keys. The public key of the receiving User Agent is used to encrypt the DES key employed in the

message encryption. The sending User Agent transfers this encrypted DES key to the receiving UA. The X.509 Directory Authentication framework is used for the authentication of the public keys of the users.

Authentication Protocol

As discussed earlier, the provision of the three services : Message Origin Authentication, Content Integrity and Non-Repudiation of Origin are grouped together.

The message-origin-authentication service is provided by the existence of message token which contains a signature which uniquely identifies the origin of the message. However, this does not guarantee that there has been no modification of the message. To achieve this, the *content integrity check* is included in the signed data part of the token.

The receiver obtains the trusted copy of the public key from the CA of the sender. If the CAs of the sender and the receiver are different, the receiver uses the certification path that has been supplied as part of the originator's certificate, to determine the copy of the receiver CA's public key. Using this, the receiver validates the signature on the originator's certificate.

The Protocol

The protocol is a slight modification of the existing X.509 Directory mutual authentication protocol [6].

step 1

The exchange between the two parties A and B with A sending message to the Authentication Server AS (in this application the Third Party) to find the public key of B [2]. This is done by looking into the database of the Directory.

$$A \rightarrow AS : A.B$$

Step 2.

$$AS \rightarrow A : D_1.D_2$$

where $D_1 = D(k^s_{AS}, A.k^p_a.t_1.t_2)$

$D_2 = D(k^s_{AS}, B.k^p_b.t'_1.t'_2)$,

t_1, t'_1 are timestamps, t_2, t'_2 are the lifetime of the corresponding keys and . indicates concatenation. In order to sign data, the user applies a one-way hash function to the data followed by his digital signature (private transformation) D. The timestamps are needed to guard against the replay attack [3]. An intruder is not able to replace the messages in the previous steps since he does not have the secret key of the AS.

Step 3.

$A \rightarrow B : D_1.R_A.B.data^1_a.E(k^p_b, data^2_a).D(k^s_a,$

$h(R_A.B.data^1_a.E(k^p_b, data^2_a)))$

where R_A is nonce chosen by A, h is strong one way hash function, $data^1_a$ is the plaintext data which they sign to preserve the integrity and $data^2_a$ is the secret data to be exchanged between the two principals A and B.

step 4.

$B \rightarrow A : R_B.A.R_A.data^1_b.E(k^p_a, data^2_b).$

$D(k^s_b.h(R_B.A.R_A.data^1_b.E(k^p_a, data^2_b)))$

where R_B is nonce generated by B, $data^1_b$ is the plaintext data and $data^2_b$ is the secret data to be exchanged.

step 5.

$A \rightarrow B : R_B.D(k^s_a.h(R_B, B))$

Thus at the end of the protocol, both the users are convinced that they are communicating with the right person. The above authentication process safeguards the integrity as well as confidentiality of the message. The users can

then generate a session key which is used to encrypt the subsequent traffic on the association.

Non-Repudiation of Delivery

The sender of the message requests this service from the receiver by including a proof-of-delivery-request flag as a part of the signed-data in the message token to the receiver. The proof-of-delivery is computed as a signature on the unencrypted message-content and the various other parameters. The receiver then returns the proof-of-delivery, together with his certificate, to the sender of the message.

Access Control Mechanisms

In this paper we will consider the access control between a User Agent and its corresponding Message Store. This is achieved by using another type of token called a *bind-token* which is exchanged between the UA and the MS at the time of connection initiation. The token includes information as signed data and time which is checked by the MS to determine if it is valid. The token signature is computed using the UA's secret RSA key. The MS then returns the token to the UA which makes further checks and if all these checks are satisfied, then the connection can be established. The token from the MS to the UA is signed which implies that the MS needs to have its own RSA pair [9, 17].

Message Loss

Vulnerability to the message loss is considered critical to the EDI application. The types of message loss can be distinguished as :

- failure of the UA or MS

- loss of individual message due to security violations.

So the transfer of messages between responsibility domains requires protection for service providers in addition to that of end users.

A.4 Summary

This paper specifies a model for a secure direct store delivery system. It is straightforward model which provides a high degree of security in a cost effective manner and has many desirable features. Particularly, if the third party provides the directory services, then electronic transactions can be carried out with a reasonable degree of security over the network. It relieves the user from burden of maintenance, upgradation of the system and expansion to other networks. Furthermore, once the user authentication is complete, all security features of the direct store delivery system will be transparent to the user.

The system makes no assumptions about the reliability of the underlying network. The data is transmitted in an encrypted form to ensure that even a third party cannot extract any information enroute. For this appropriate end-to-end encryption must be provided to counter traffic analysis.

Acknowledgments

We would like to thank the anonymous referees for ACSC'95 for their helpful comments. The second author was supported in part by ARC A49232172, ATERB N069/412 and a University of Wollongong Research Program grant.